



Veeva Network MDM

Veeva Network MDM 26R2.0 Early Release Notes

July 2026



Contents

About these Release Notes	8
Release dates	8
Subscribe to release notifications	8
Software releases and maintenance	8
Release Notes and Data Governance documents	8
Browser requirements	8
What's new.....	9
Announcements.....	12
New fields enabled by default.....	12
Fields for unmerged records.....	12
New field for OpenData 2.0	13
Considerations for existing Network MDM instances.	14
General	15
Maps.....	15
Product name.....	16
Updates	16
Hierarchy Explorer widget.....	17
Access from HCP accounts in Vault CRM	17
Widget access	18
Exporting hierarchies	18
Hide Export to Excel.....	18
Existing property.....	19
Data change requests.....	20
Master data disclaimer	20



Impacted records.....	20
Required confirmations	20
Supported DCRs.....	20
Confirming the DCR data	21
Send to OpenData	21
Change Request API updates.....	22
Logs.....	24
Search.....	25
Improved phonetic search	25
Profiles	27
Profile Inspector	27
Supported users.....	27
Supported records	27
Display on profiles	28
Using Profile Inspector	28
Sections	29
Search for fields	29
Parent HCO enhancements.....	31
Key details	32
Available actions.....	32
OpenData 2.0 data model	33
License support	33
Enable License fields for OpenData 2.0	33
Receive License and Identifier data from OpenData	34
License fields.....	36



Identifiers	38
Support for Identifier data.....	39
Defining Identifiers	39
Profile layouts.....	40
Identifiers on record profiles.....	42
Adding and updating identifiers	44
Data change requests	45
Considerations for other features	47
IQVIA OneKey Connector	48
Processing IQVIA reference data.....	48
OneKey reference data file	48
Supported actions.....	49
Reference update job	50
Simulation mode	52
Unmerge OneKey records	53
Unmerged records file.....	53
About the unmerge job process	54
Unmerged records.....	54
Integration Dashboard	54
IQVIA OneKey configurations	55
Data model	57
New fields for unmerged records	57
Benefits.....	57
New fields	58
Supported records	58



About unmerged records	58
View the fields on record profiles.....	60
Unmerged fields on OpenData records	60
Report on unmerges.....	61
Cluster management.....	62
Update addresses	62
OpenData subscriptions	63
Advanced filters	63
Filter options.....	64
Create an advanced filter	64
Query validation	68
Managed filters.....	69
Updates for field management	71
Enhanced job details	72
Processed records.....	72
Primary CDA address field.....	73
Data impact	73
Update the field.....	73
Subscriptions	75
Country visibility for jobs	75
Supported jobs	75
Country details	75
Country details	76
Source subscriptions	77
Advanced properties for reference data updates.....	77



Integrations	78
Event streams.....	78
Benefits.....	78
Comparison of export patterns	78
How event streams work.....	79
Supported changes	79
Getting started	79
Create an Integration user.....	80
Define an event stream	81
Preview the event stream	85
Develop the consumer	87
Offset management.....	88
Avoid duplicating data across streams	90
Turn off an event stream	90
Vault CRM credential	91
About the Network System User in Vault CRM	91
New Vault CRM implementations	91
Existing Vault CRM implementations	92
Prerequisite tasks for the Network System User.....	92
Create a Vault CRM credential	92
Update the Vault CRM Bridge.....	95
Switch to the Network System User	96
Security.....	97
Dynamic user provisioning for Single Sign-On (SSO)	97
Highlights	98



Updates for SAML mappings	98
Upload a file of your group mappings	101
Mapping rules.....	105
Updating the mappings	106
Test the SSO configuration	107
Logs.....	108
SSL certificate update.....	108
API.....	109
Version Update for 26R2.0.....	109
Version Update for 26R1.1.....	109
Restrict access to authorized systems.....	109
Access to systems	110



About these Release Notes

These Release Notes describe all features that will be included in Veeva Network MDM 26R2.0.

RELEASE DATES

- **Sandbox release** (version 26R2.0) - Friday, August 7
- **Production release** (version 26R2.0.1) - Friday, August 21

SUBSCRIBE TO RELEASE NOTIFICATIONS

You can receive email notifications about upcoming software releases and the supporting documentation.

Software releases and maintenance

- [Veeva Trust Site](#)

At the top of the page, click **Subscribe to Veeva Trust Site** and subscribe to the Veeva Network MDM component.

Release Notes and Data Governance documents

The documents are posted in the following locations:

- Veeva Connect - Join the [Network MDM Community](#).

To be notified as soon as the Release Notes are posted, go to your Veeva Connect profile and click **Settings**. On the Email Frequency page, expand the list and choose **Immediate**. Other notification options are **Daily** and **Weekly**.

- [Veeva Network MDM Online Help](#)

For more release information, see [About Network MDM Releases](#) in the *Veeva Network MDM Online Help*.

Browser requirements

Veeva Network MDM is supported on the latest version of these browsers, as of their most stable version at the time of release:

- Google Chrome™
- Apple® Safari®
- Microsoft® Edge

Veeva Network MDM is not supported on mobile devices.



What's new

The following key enhancements comprise the Veeva Network MDM 26R2.0 major release.

			ST	DS	DM	AD
Announcement						
New fields enabled by default	To support enhancements in version 26R2.0, several new fields will be added and enabled by default in all Network MDM instances.	26R2.0	•	•	•	•
General						
Map updates	Style updates have been made to maps on record profiles to align with search and geocoding changes.	26R2.0	•	•	•	•
Product name	The user interface is now rebranded with the Network MDM product name.	26R1.1	•	•	•	•
Hierarchy Explorer widget						
Access from HCP accounts in Vault CRM	When the Hierarchy Explorer widget is embedded in Vault CRM, end users can now access the widget directly from an HCP account.	26R2.0	•	•	•	•
Export to Excel	Administrators can disable the option to export hierarchies to a Microsoft Excel file.	26R1.1	•	•	•	•
Data Change Requests						
Master data disclaimer	Users must confirm that DCR updates for mastered records do not come from external data sources.	26R1.1	•	•	•	•
Search						
Improved phonetic search	Search behavior has been expanded to support a broader range of alternate spellings and phonetic name variations.	26R2.0	•	•	•	•
Profiles						
Profile Inspector	The Profile Inspector is a tool that you can use to see all of a record's fields, including fields not on the profile, on a single, easy-to-search screen.	26R2.0		•	•	•
Parent Affiliation improvements	The Parent Affiliation section is updated to include pagination.	26R2.0	•	•	•	•



			ST	DS	DM	AD
OpenData 2.0 data model						
License support	The data model is extended to support the License object which includes the Identifier component.	26R2.0	•	•	•	•
Identifiers	Identifier data (for example, NPI numbers and VAT IDs) is now stored as a License component rather than fixed fields, allowing you to assign multiple ID types to a single record to support complex business scenarios.	26R2.0	•	•	•	•
IQVIA® OneKey data						
Process IQVIA reference data	IQVIA custom reference field value lists in Network MDM are updated with the latest reference data provided by IQVIA.	26R1.1			•	•
Unmerge records	Network MDM can now unmerge OneKey records during the source subscription job.	26R1.1			•	•
Integration Dashboard	The IQVIA OneKey system is included in the dashboard.	26R1.1				•
Data Model						
New fields for unmerged records	To help users more easily track record unmerges, new fields are added to unmerged records so its history can be viewed directly on the record.	26R2.0			•	•
Cluster management	Updated codes are available for Spain and the UK.	26R1.1			•	•
OpenData Subscriptions						
Advanced filters	Administrators can define advanced filters using SQL queries to specify additional records to download in country subscriptions.	26R2.0			•	•
Updates for field management	Subscription settings are updated with clearer field labels making it easier for Data Managers to understand and select which fields are managed by OpenData.	26R2.0			•	•
Enhanced job details	The Job Result Summary now includes a new column that displays the total count of processed records.	26R2.0			•	•
Primary CDA address field	Administrators can configure the Primary CDA field to be OpenData-managed in country subscriptions.	26R1.1			•	•



			ST	DS	DM	AD
Subscriptions						
Track countries	Data managers can see the countries impacted by jobs.	26R2.0				•
Source Subscriptions						
Reference data issues	Administrators can configure subscriptions to update records even though reference data issues are identified.	26R1.1			•	•
Integrations						
Event Streams	Event Streams is a new integration pattern that you can use to immediately notify downstream systems about time and business critical updates.	26R2.0			•	•
Vault CRM	A new Vault CRM credential supports the Network System User that is now provisioned in each Vault CRM instance.	26R2.0				•
Security						
Dynamic user provisioning for single sign-on (SSO)	Administrators can now use their SSO provider groups and countries to automatically set up new users with the right access and settings the first time they log in.	26R2.0				•
SSL certificate updates	Customers who explicitly download and install certificates must update the certificate for veevanetwork.com.	26R2.0				•
API						
Version update - 26R2	The Network MDM API is updated to v40.0.	26R2.0				Developers
Version update - 26R1.1	The Network MDM API was updated to v39.0.	26R1.1				Developers
Restrict access to authorized systems	The Change Request Search and Retrieve APIs now enforce the system access restrictions in your user profile.	26R1.1				•

Note: The System and Data Admin user has all of the capabilities of the System Administrator and Data Steward users. Features and enhancements that apply to those users also apply to the System and Data Admin user.

Data Governance - Specific updates for fields and reference data are provided in the [Veeva Network MDM Data Governance](#) release notes for every minor and major Network release.



Announcements

NEW FIELDS ENABLED BY DEFAULT

To support enhancements in version 26R2.0, four new fields will be added and enabled by default.

Fields that are enabled by default can impact your current configurations. Evaluate any potential impact before 26R2.0 is released to your Sandbox and Production Network MDM instance.

Fields for unmerged records

The following system fields have been added to HCO, HCP and custom main objects to provide additional details on unmerged records.

Field Name	Label	Description
record_unmerged_date__v	Unmerged Date	Date when the record was unmerged.
record_unmerged_from_vid__v	Unmerged from Network ID	Network ID of record that this record was unmerged from
record_unmerged_original_vids__v	Unmerged Original Record Network IDs	The Network IDs of the records that existed before they were merged. It confirms which original record's data is now being restored into the new record.

Supported countries

- All countries

Field details

Managed by OpenData?	Yes
Enabled by default?	Yes, for all Network MDM instances.
Immediate data impact?	Yes
Profile layouts	The fields will be added to standard layouts. They must be added to custom profile layouts.

For information about the enhancement, see the [New fields for unmerged records](#) topic.



New field for OpenData 2.0

Support for License sub-objects is being added in this release. Licenses now also include a separate component for Identifier data (for example, NPI numbers in the US and Tax IDs in Europe).

A new field will be added to the License object and enabled by default to define a License record as either a "License" or an "Identifier".

Field Name	Field Label	Field Type	Description
object_cat_type__v	Object Category Type	Reference Type	This is an important field that determines if the record is a License or an Identifier. Possible values: LICENSE, ID or no value (for existing Licenses). The default value for new records is LICENSE.

Supported countries

All countries/regions except the following:

- Belarus
- Burkina Faso
- China
- Ethiopia
- Hong Kong
- Iraq
- Japan
- Macao
- Madagascar
- Mali
- Sierra Leone
- Russia
- Tajikistan
- Turkmenistan
- Uzbekistan
- ZZ (All Other Countries)

Field details

Managed by OpenData?	Yes
Enabled by default?	Yes, for all Network MDM instances.
Immediate data impact?	Yes
Profile layouts	The field will be added to the GlobalStandard layout for HCPs and HCOs. It must be added to custom profile layouts. No impact or action required to custom layouts if you do not use the OpenData 2.0 data model or the Identifier for Licenses.

For information about the enhancement, see the [OpenData 2.0 data model](#) topic.



Considerations for existing Network MDM instances.

When fields are enabled by default, it can impact target exports and reporting.

- **Target Exports** - New fields will automatically be included in target subscriptions configured to export all objects and fields.
- **Reporting** – Queries or saved reports using SELECT * will return different results.

Action required to prepare for these fields

Before the fields are added in this release, the following tasks should be considered:

- **Audit Downstream Systems** - Identify target exports that pull "all fields" and either update downstream systems to accept the new data or limit the subscription to specific fields only.
- **Review Custom Reports** - Update any SELECT * reporting queries to use explicit field names instead, if those reports don't require these fields.
- **Plan Configuration Updates** - Add tasks to your 26R2.0 release checklist to update custom profile layouts if you plan to use this data.



General

MAPS

26R2

Maps across all Network MDM features have been updated with subtle design refreshes and changes for geocoded addresses.

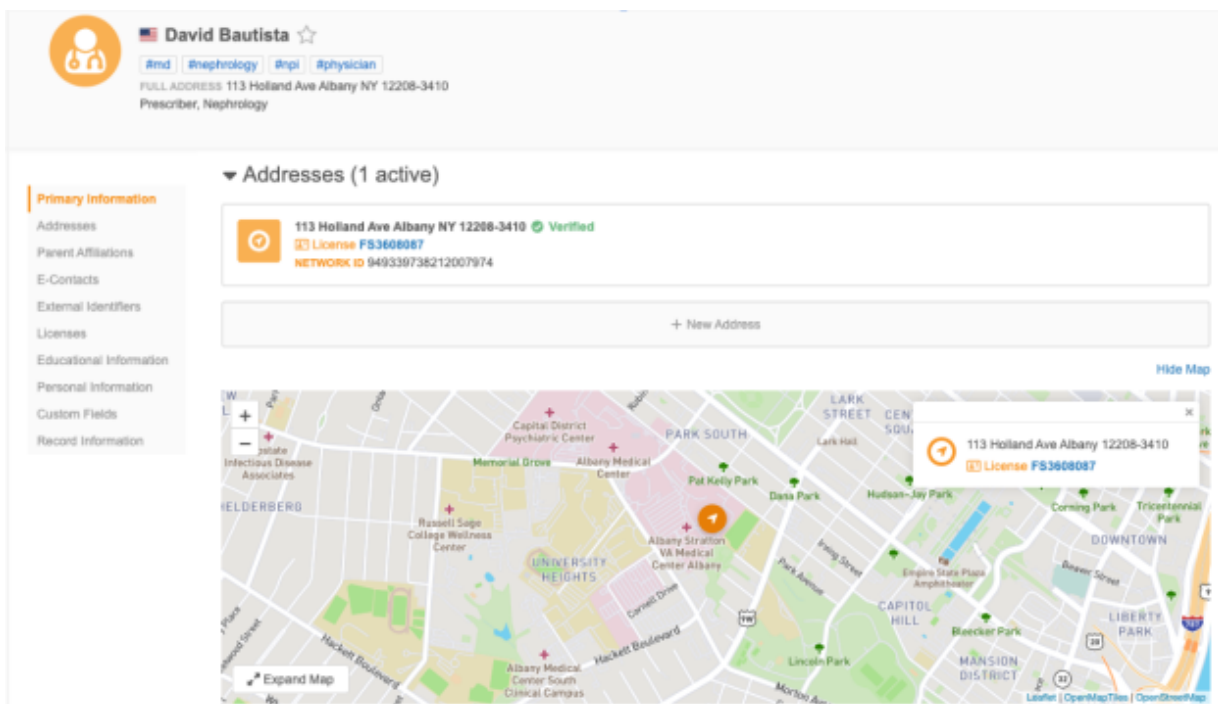
These enhancements are enabled by default.

Maps are available in the following features:

- Network Search
- Profile page
- Network Explorer
- Admin Homepage

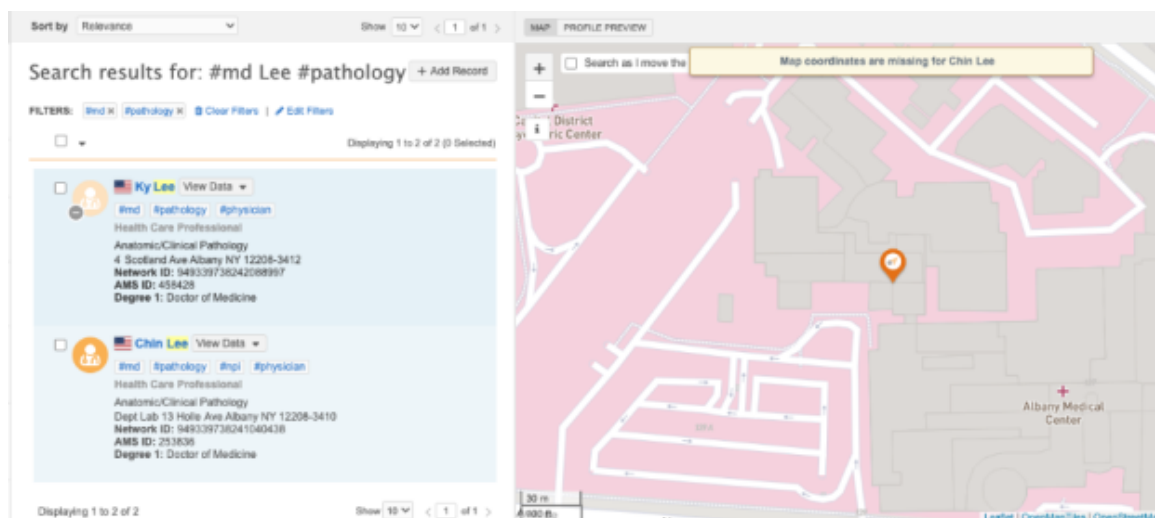
Users will notice the following changes:

- **Style** - Minor changes in visual styling to the map interface.



- **Geocoding** - Addresses without latitude and longitude coordinates will not display on maps.

If an address cannot be mapped, the following message displays: `Map coordinates are missing for <record name>`.

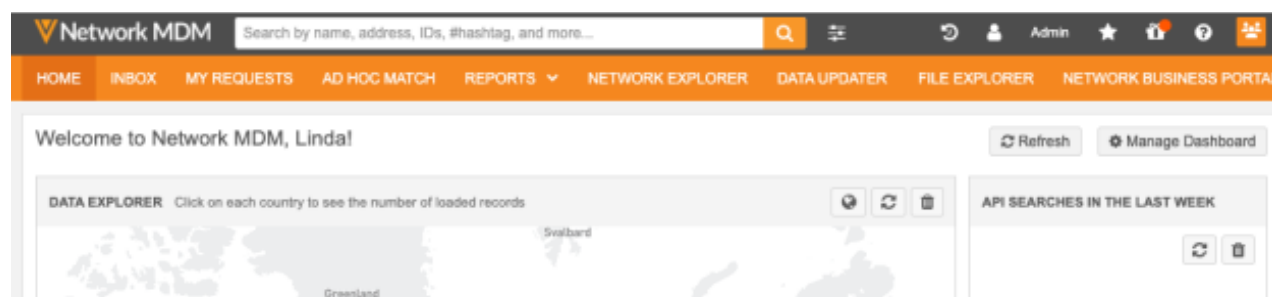


PRODUCT NAME

26R1.1

Veeva Network is now Veeva Network MDM. This new name highlights its power as a multi-domain master data management platform and customer master application that can be used with any reference data provider.

The rebranded product name now displays in the Network MDM user interface.



This enhancement is enabled by default.

Updates

The updates are made to logos and labels in the Network MDM user interface.

The rebranded product name does not impact your instance names, feature configurations, or reporting.



Hierarchy Explorer widget

Hierarchy Explorer is a Network widget that you can use to see all levels of an HCO's structure, making it easy to visualize their hierarchy and find new targets.

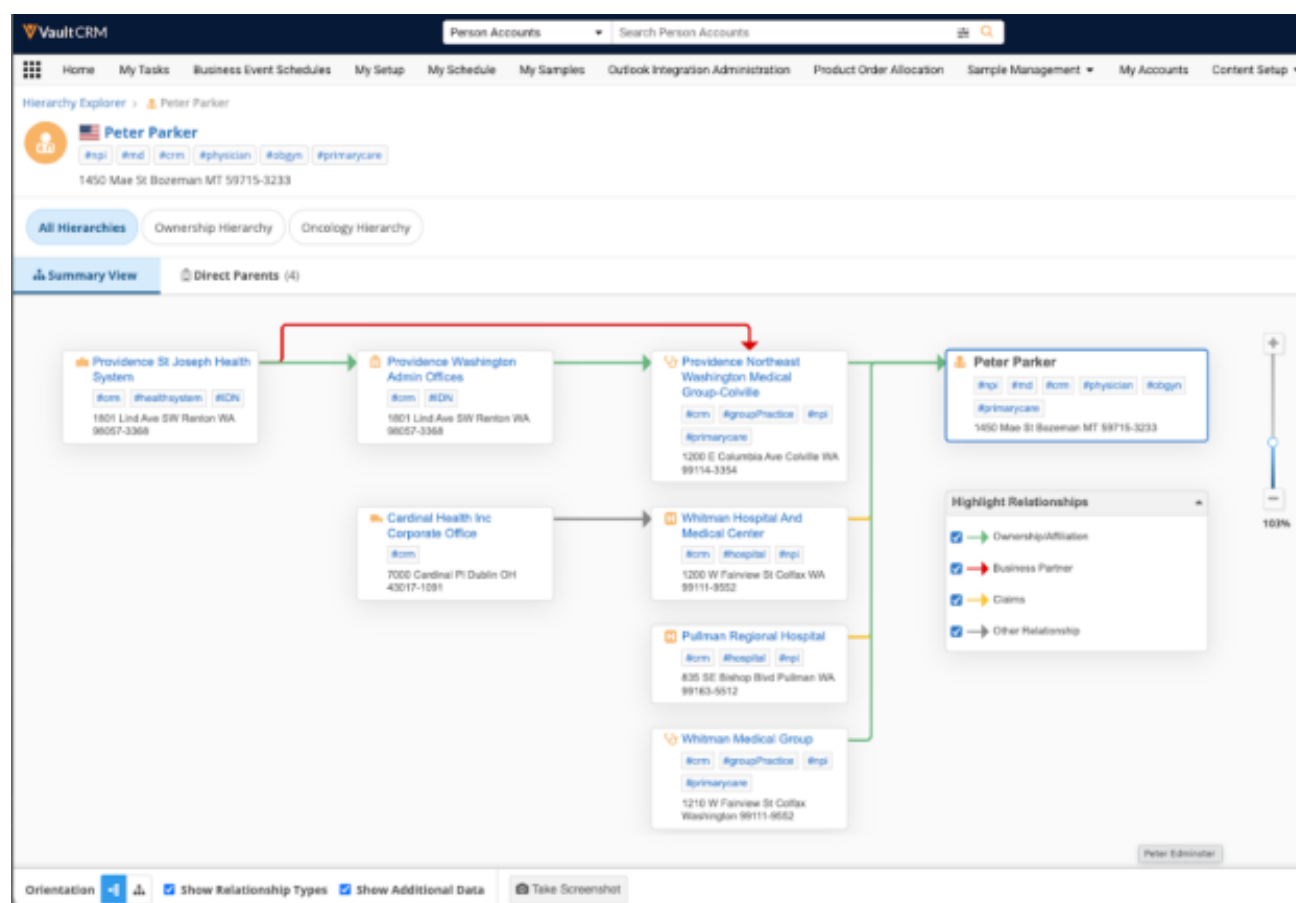
To enable Hierarchy Explorer in your Network MDM instance, contact Veeva Support.

The following enhancement has been added for the Hierarchy Explorer widget in this release.

ACCESS FROM HCP ACCOUNTS IN VAULT CRM

26R2

When the Hierarchy Explorer widget is embedded in Vault CRM, end users can now access the widget directly from an HCP account. Previously, Hierarchy Explorer could be accessed from HCO accounts.



This enhancement is available by default if the widget is embedded in Vault CRM. For details, see the [Network Hierarchy Explorer](#) topic in the *Vault CRM Online Help*.



Widget access

Vault CRM users can access the widget when they are logged in using their Vault credentials. On an HCP Account page, click **More Actions** and select **Network Hierarchy Explorer**.

The HCP's hierarchy opens so users can immediately explore it. Users can also submit data change requests through the widget.

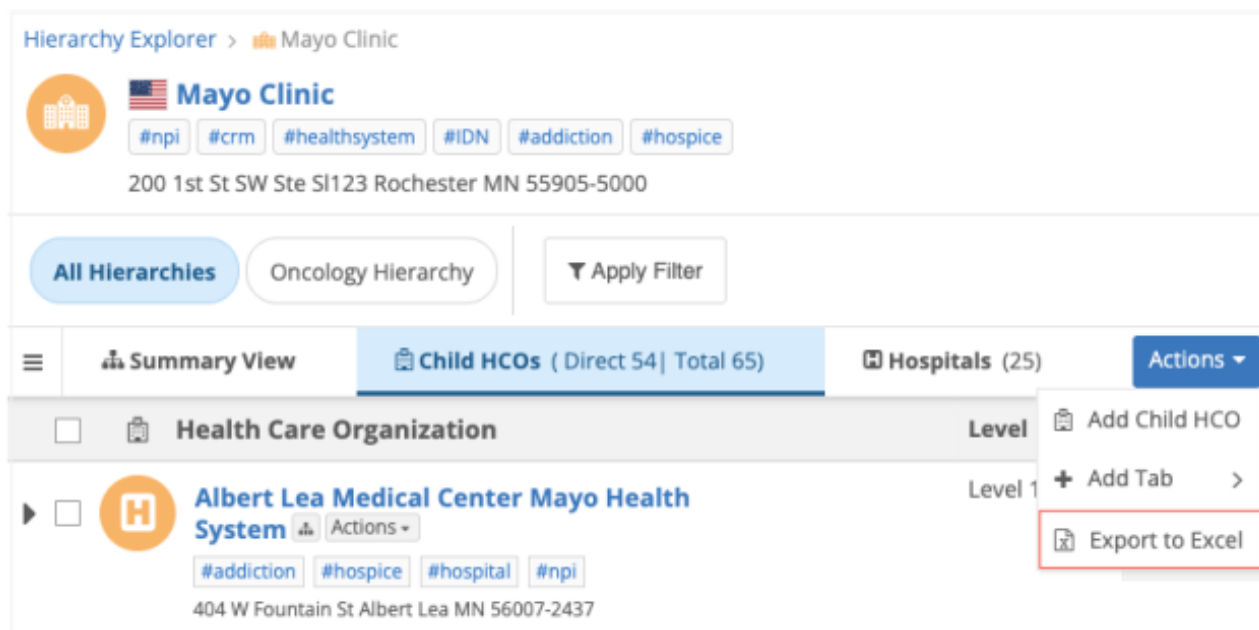
For information about configuring the widget for Vault CRM, see [Embed Hierarchy Explorer in Vault CRM](#) in the *Veeva Network MDM Online Help*.

EXPORTING HIERARCHIES

26R1.1

The option to export the hierarchy to a Microsoft Excel file is available from the **Child HCPs**, **Child HCOs**, and custom tabs. For compliance, it might be necessary to prevent users from exporting HCP and HCO details from the widget. Administrators can now configure the widget to hide the **Export to Excel** option from the **Actions** menu on these tabs.

This can be applied to Hierarchy Explorer embedded in Vault CRM.



This enhancement is available by default in your Hierarchy Explorer configuration. The **Export to Excel** option displays by default for widgets.

Hide Export to Excel

1. Open a Hierarchy Explorer widget configuration (**Widgets & Portal > Network Widgets**).
2. In the **General Settings** section, a new heading, **Export to Excel Settings** displays.
3. Clear the **Display Export to Excel option** setting. It is enabled by default.



SUMMARY VIEW SETTINGS

Define how Summary View tab displays in your widget.

☐ Set the Summary View tab as the first tab in Hierarchy Explorer

☐ Display relationship types in Summary View by default

EXPORT TO EXCEL SETTINGS

Enable this option to allow users to export records from the Hierarchy Explorer to Excel.

☒ Display Export to Excel option

4. **Save** your changes.

Existing property

Previously, the **Export to Excel** option could be hidden using a widget property in your internal application or through a setting in the Network Portal.

If you are already using the property in your widget code (`hide-export-button="true"`) or the setting in the Network Portal, the **Export to Excel** option will not display in the widget.



Data change requests

MASTER DATA DISCLAIMER

26R1.1

For compliance, you must now confirm that the new information you are submitting in a data change request was not sourced from another master data provider. This ensures that data that you license from another provider is not shared with another master provider.

The following message displays when you submit a change to a mastered field on a mastered record.

Disclaimer

I confirm that the information I am submitting is based on my personal observations, research or interactions with an HCP/HCO, and is not based on any information my company licensed from another data provider.

This enhancement is enabled by default in your Network MDM instance.

Impacted records

The confirmation applies to records owned by the following master data providers:

- Veeva OpenData
- IQVIA® OneKey
- Other third-party data providers

Required confirmations

The disclaimer displays only when you submit a change to a mastered field that is routed to a master data provider.

Record Owner	DCR Fields	Confirmation Required?
OpenData	OpenData	Yes
OpenData	OpenData and Custom	Yes
OpenData	Customer	No
Third Party	Third Party	Yes
Third Party	Third Party and Custom	Yes
Third Party	Custom	No
Locally managed	Custom	No

Supported DCRs

- Add Requests
- Change requests



Confirming the DCR data

When you submit a change on a mastered record, the confirmation displays when you apply the change. You must confirm when you submit an add or change request through the following methods:

- Profile page
- Network widgets (Search, Profile, Hierarchy Explorer)

Example DCR submitted from the Profile page

On the Profile page, the confirmation displays on the **Apply Change Request** dialog.

Apply Change Request [X]

You have made a change to OpenData data, Veeva data stewards will review this change as soon as possible

Notes

Attachments

You are about to upload an attachment to support a Data Change Request. By uploading, you confirm that the attachment contains HCO/ HCP contact details that you collected from publicly available or accessible sources. Only image file types will be accepted. Images shall not contain people or any offensive content. Attach up to 3 photos to your change request. File size limit: 0MB per file

Browse Files

Disclaimer *

☐ I confirm that the information I am submitting is based on my personal observations, research, or interactions with an HCP/HCO, and is not based on any information my company licensed from another data provider.

Cancel Apply

Select the checkbox to confirm that the data did not originate from another data source. The **Apply** button is not active until the confirmation is applied.

Send to OpenData

Local data stewards must confirm that they are not including third-party data when they send a record to OpenData to start mastering.

The **Send to OpenData** button is not active until the confirmation is applied.



Confirm Send to OpenData

Requestor Notes

Please provide additional information to assist in approval process for the request.

Attachments

You are about to upload an attachment to support a Data Change Request. By uploading, you confirm that the attachment contains HCO/HCP contact details that you collected from publicly available or accessible sources.

Only image file types will be accepted. Images shall not contain people or any offensive content.

Attach up to 3 photos to your change request. File size limit: 20MB per file

Browse Files

Disclaimer *

You are attempting to send data to Veeva as part of an add request, and this data will become an OpenData record once validated.

☐ I confirm that the information I am submitting is based on my personal observations, research, or interactions with an HCP/HCO, and is not based on any information my company licensed from another data provider.

Cancel

Send to OpenData

Change Request API updates

The Change Request API contains a new parameter to identify the master data confirmation:

- **source_verified**

Integration users should submit DCRs with the **source_verified** parameter to confirm that data in the DCR is not from another data provider.

Supported values

Value	Outcome
true	The DCR is routed to the appropriate master to be processed. Note: If the source_verified value is not defined, the DCR outcome is the same as <i>true</i>. However, it will not be logged in the Task Audit Log because there is no value.
false	The DCR on existing master managed fields are auto-rejected. If Review Rejections is on (Workflow Settings), a new add request or new sub-object is routed to local data stewards.



API version

The **source_verified** parameter is supported for Network API version 39.0. If the parameter is used in earlier API versions, it is ignored.

Example request

```
POST https://my.veevanetwork/api/v39.0/change_request/search?source_verified=true
```

Example response

```
{
  "change_request_id": "949198485141127199",
  "status__v": "CHANGE_PENDINGREVIEW",
  "result__v": null,
  "entity_type": "HCP",
  "vid_key": null,
  "vid__v": null,
  "metadata": {
    "creator": "crmuser@verteo.veevanetwork.com",
    "note": "John Smith is a new doctor at Memorial Hospital",
    "source": "Veeva CRM",
    "system": null
  },
  "resolution_notes": null,
  "entity": {
    "object_id": "949198485140668447",
    "object_name": "HCP",
    "first_name__v": {
      "change_requested": "John",
      "final_value": null,
      "result": null
    },
    "last_name__v": {
      "change_requested": "Smith",
      "final_value": null,
      "result": null
    },
    "primary_country__v": {
      "change_requested": "US",
      "final_value": null,
      "result": null
    }
  },
  "source_verified": "true",
  "created_date": "2026-06-26T10:51:51.000-04:00",
  "completed_date": null,
  "taskCountry": "US",
  "task_type": "ADD_REQUEST",
  "original_task_type": "ADD_REQUEST",
  "parent_task_ids": [],
  "reserved_vid": null
}
```

The Search Change Request and Retrieve Change Request responses contain the **source_verified** value if the parameter was submitted in the DCR.



Logs

Administrators can track the master data confirmation responses using the Task Audit History (**Logs**).

A new **Action Type** is created to identify the response for all DCRs.

ActionType	Message
RouteToLocal	Source not verified. Route to local stewardship.

Example

Task Audit History

Export

Date range

To

2026-05-26

2026-05-27

Get History

Reset

Choose time period...

Showing events for 2026-05-26 to 2026-05-27

ID	TASK ID	ACTION DATE	ACTION TYPE	USER NAME	RELATED ITEMS	MESSAGE
2234	949022547123899551	2026-05-26 14:08:31 IST	IncrementDeltaId	System	DCR ID: 949022547123899551 Entity ID: 243230539576771592	Incremented delta id of entity 2432...
2233	949022547123899551	2026-05-26 14:08:31 IST	ServiceLog	System	DCR ID: 949022547123899551 Entity ID: 243230539576771592	Auto rejected by Network System.
2232	949022547123899551	2026-05-26 14:08:30 IST	RouteToLocal	System	Source not verified. Route to local stewardship.	Source not verified. Route to local ...
2231	949022547123899551	2026-05-26 14:08:30 IST	ServiceLog	System	DCR ID: 949022547123899551 Entity ID: 243230539576771592	Auto rejected by Network System.



Search Term	Previous Results	New Results
Norany	Results may not be returned. Sort byRelevance Search results for: norany Didn't find what you were looking for? Try Advanced Search. ☐ No Results Displaying 0 to 0 of 0	Norlan, Nurani, Noland, Noorani Sort byRelevance Search results for: Norany Didn't find what you were looking for? Try Advanced Search. ☐ ☐   Isla Norlan View ta #md #npi #physician #psych Health Care Professional Psychiatry 790 Fuller Ave NE Grand Rapids MI 49503-1918 Specialty 1: Psychiatry ☐   Doctor Nurani Sivaram View Data #dr #gastro #primarycare #specialist #srd Health Care Professional Gastroenterology, Internal Medicine Eiland Lane Eiland HX5 9EB Calderdale Specialty 1: Gastroenterology ☐   Shea Noland View ata #md #npi #orthosurg #physician #plasticsurg Health Care Professional Plastic Surgery, Hand Surgery 5777 E Mayo Blvd Phoenix AZ 85054-4502 Specialty 1: Plastic Surgery ☐   Fama Noorani View Data #md #npi #physician #psych Health Care Professional Psychiatry 2120 L St NW Ste 600 Washington DC 20037-1540 Specialty 1: Psychiatry ☐   Ross Noland View Data #nurse Health Care Professional

This enhancement is enabled by default.



Profiles

PROFILE INSPECTOR

26R2

The Profile Inspector is a tool that you can use to see all of a record's fields, including fields not on the profile, on a single, easy-to-search screen. Data Stewards can use the view to quickly find fields without digging into the different sections on the Profile page.

The screenshot shows the Network MDM Profile Inspector interface. The top navigation bar includes 'HOME', 'INBOX', 'MY REQUESTS', 'AD HOC MATCH', 'REPORTS', 'NETWORK EXPLORER', 'DATA UPDATER', 'FILE EXPLORER', and 'NETWORK BUSINESS PORTAL'. The main content area is titled 'Recent > Roswell Park Comprehensive Cancer Center'. It features a sidebar with 'Primary Information' and a list of categories: Addresses, Parent HCO Affiliations, Child Affiliations, OpenData Hierarchy, General Information, External Identifiers, Licenses, and Record Information. The main area displays a table of fields and their values, with a search bar at the top. The table includes fields like '# of non-MDs and DOs all locations', 'Accept Medicaid?', 'Accept Medicare?', 'AMA Do Not Contact?', 'American Hospital Association ID', 'AMS ID', 'Associated with Kaiser?', 'Candidate Record', 'City (CDA)', 'CMS Certification #', 'Communication', 'Corporate Name', 'Created Date', 'Delta ID', 'Entity Type', and 'Externally Mastered Record?'. The values are displayed in a table format.

This feature is enabled by default for your Network MDM instance.

Supported users

- Data Stewards
- Data Managers
- System Administrators
- System and Data Admins

Supported records

- **Type** - HCPs, HCO, custom objects
- **Ownership** - Locally managed, Veeva-managed, and third-party managed records.

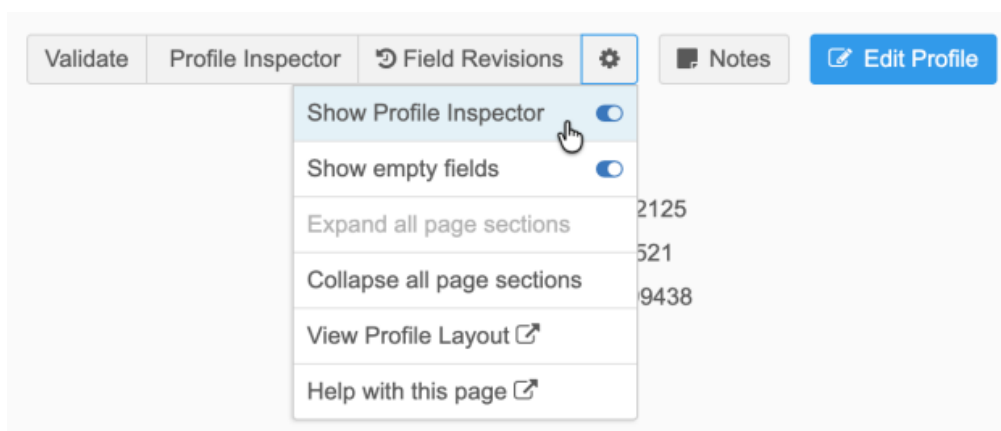
Profile Inspector can also be used on records not yet downloaded from OpenData.



Display on profiles

The **Profile Inspector** button does not display by default on record profiles. Users can choose to display the button.

- Expand the **More Options** menu and toggle the **Show Profile Inspector** option to On. Your preference is remembered the next time you visit a record profile.



Using Profile Inspector

On any record, click **Profile Inspector** to open the tool.

Available fields

Profile Inspector includes all fields and values for that record, including fields that do not display on the Profile page.

A **Metadata** tag is added beside fields that are not part of the data model but are added to help users understand the record; for example, the `corporate_name__v` field is added to parentHCO records.

- **Display order** - The fields display in alphabetical order.
- **Field color** - The color indicates field management if you have the **Field Ownership** option selected (**More Options** menu).
- **Multivalued fields** - Fields with multiple values display as comma-separated lists.
- **Copy** - A **Copy** icon displays beside each field.



Sections

Separate sections display for sub-objects. Click the section name, for example **Addresses** or **ParentHCOs**, to jump to that section in the tool.

Each section can be expanded or collapsed.

The screenshot shows the Profile Inspector tool interface. At the top, there is a search bar labeled "Filter fields or values...". Below it, a "Jump To:" section contains links for "Addresses (7)", "Custom Keys (1)", "Licenses (1)", and "Parent HCOs (2)". The main content area is titled "Set of Parent HCOs (parent_hcos__v)". On the right, a record is displayed for "Record: 928644902633668652 ~ Kaleida Health Admin". The record details are as follows:

Field	Value
Candidate Record (candidate_record__v) metadata	false
Corporate Name (corporate_name__v) metadata	Kaleida Health Admin
Created Date (created_date__v)	2024-12-17 11:39:58
Data Provider Primary Relationship (is_primary_relationship__v)	No/False (N)
Delta ID (record_delta_id__v)	946050708325498879
Entity Type (entity_type__v)	Health Care Organization (HCO)
Entity Type of the related object (related_entity_type__v) metadata	Health Care Organization (HCO)
Externally Mastered Record? (is_externally_mastered__v)	false
Full Address (formatted_address__v) metadata	100 High St Buffalo NY 14203-1126
HCO Type (hco_type__v) metadata	Organization, Admin Only (4:11)
Hierarchy Type (hierarchy_type__v)	Operating/Ownership Hierarchy (HCO_HCO)
Modified Date (modified_date__v)	2024-12-17 11:50:48

Search for fields

Use the **Search** bar to quickly find specific data points, for example, field labels and names, reference labels and values.

If you filter the record for a specific search term, your preference is remembered the next time you open Profile Inspector on any record.



Example

Search for "primary" to see all fields on the record that are set to primary.

primary

×

Jump To: [Addresses \(7\)](#) [Communications Sub-Objects \(3\)](#) [Custom Keys \(4\)](#) [Licenses \(3\)](#) [Parent HCOs \(3\)](#)

Primary Country (primary_country__v)	United States (US)
Primary Specialty Group (primary_specialty_group__v)	Anesthesiology (G-AN)
Set of Addresses (addresses__v)	Record: 243372145395106824 ~ 555 Knowles Dr Los Gatos California 95032-1549 ⓘ Primary (CDA) (primary_cda__v) Yes/True (Y) primary address (primary_address__c) Yes/True (Y) Primary Zip/Postal Code (postal_code_primary__v) 95032 Record: 243372145395106819 ~ 5593 Perugia Cir San Jose CA 95138-2338 ⓘ Primary Zip/Postal Code (postal_code_primary__v) 95138 Record: 928944441110890408 ~ John G Kelley Md Perugia Cir MSC 5593 San Jose CA 95150-5593 ⓘ Primary Zip/Postal Code (postal_code_primary__v) 95150 Record: 243372145395106826 ~ 815 Pollard Rd Los Gatos CA 95032-1438 ⓘ Primary Zip/Postal Code (postal_code_primary__v) 95032 Record: 243372145395106828 ~ 20103 Lake Chabot Rd Castro Valley CA 94546-5305 ⓘ Primary Zip/Postal Code (postal_code_primary__v) 94546 Record: 243372145395106832 ~ 1655 Magnolia Blossom Ln San Jose CA 95124-6421 ⓘ



PARENT HCO ENHANCEMENTS

26R2

To help you find affiliations faster on records with high volumes of parent HCOs, the **Parent Affiliation** section is enhanced. You can now navigate large lists effortlessly using pagination or quickly locate affiliations using specific keywords. For example, search for the Network ID of a hospital to find it in any affiliation card on the record.

▼ Parent Affiliations (13 Active | 1 Inactive)

All Statuses Selected [Reset Filters](#)

Cardiac Testing LTD
[#cardio](#)
FI Galleria 2900 W Oklahoma Ave # 4th Milwaukee WI 53215-43
HCO TYPE Organization, Group at Hospital
RELATIONSHIP TYPE Business Partner/Affiliate
CLASS OF WORK
NETWORK ID 949141565476963937

Under Review

Gem Diagnostic Testing
[#groupPractice](#) [#podiatry](#)
755 E 49th St Ste 10 Hialeah FL 33013-1906
HCO TYPE Organization, Group Practice
RELATIONSHIP TYPE Admitting Privileges
CLASS OF WORK
NETWORK ID 949141565476963936

Under Review

Mt Sinai Cornea External Disease Refractive Surg
[#groupPractice](#) [#vision](#)
13527 38th Ave Ste 398 Flushing NY 11354-4448
HCO TYPE Organization, Group Practice
RELATIONSHIP TYPE Affiliation
CLASS OF WORK
NETWORK ID 806812069490955272

New York Eye And Ear Infirmary Of Mount Sinai
[#npi](#) [#hospital](#) [#medicare](#) [#vision](#)
310 E 14th St New York NY 10003-4201
HCO TYPE Organization, CMS Teaching Hospital
RELATIONSHIP TYPE CMS Facility Claims
CLASS OF WORK
NETWORK ID 929652465805428649

New York Eye And Ear Infirmary Of Mount Sinai
[#vision](#)
South Bldg 310 E 14th St Ste 219 New York NY 10003-4284
HCO TYPE Optical Center
RELATIONSHIP TYPE Affiliation
CLASS OF WORK
NETWORK ID 776777300023809031

Displaying 1 to 5 of 14

Show 5 1 of 3 < >

This enhancement is enabled by default.



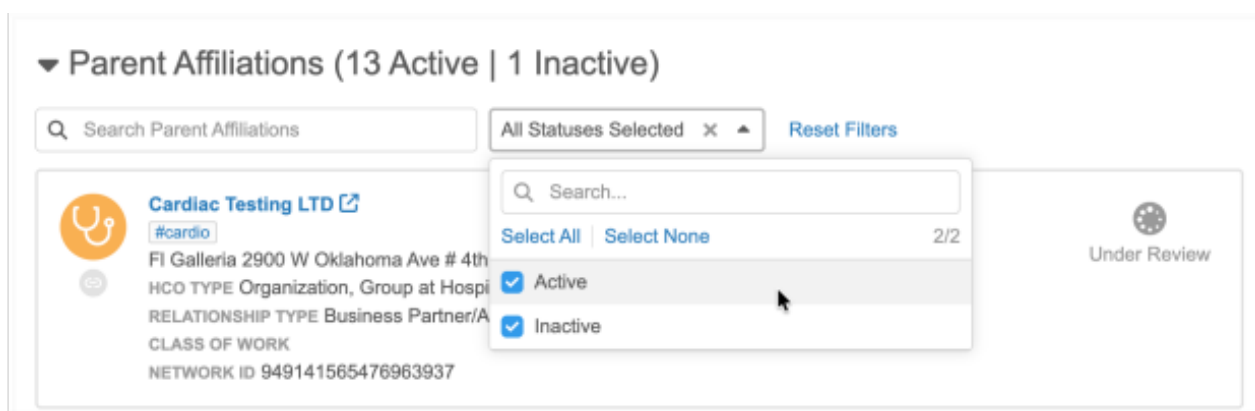
Key details

Detail	Explanation
Limit of records	A maximum of 500 affiliations can display for each record. This is an existing limit that has not changed with this enhancement.
Default number of records per page	Five records display by default. Use the Show option to change your preference to display 10 records. Your preference will be remembered the next time you visit a record profile.
Page display order	Affiliations are listed in the following order: • Primary affiliations • Active affiliations listed in alphabetical order • Inactive affiliations listed in alphabetical order. When new affiliations are added on the Profile page, they are added to the bottom of the active affiliations. If it is marked as a primary record, it will display at the top of the list.

Available actions

- **Search** - Use the Search bar to find an affiliation on any page in the section.
- **Filter** - Use the **Status** filter to display **All Statuses**, **Active**, or **Inactive** affiliations.

The filter is remembered as you visit other records or return to the Profile page.





OpenData 2.0 data model

The OpenData 2.0 data model was released in June 2026. It supported the HCO, HCP, Address, and Parent HCO objects.

The following enhancements have been added in this release.

LICENSE SUPPORT

26R2

The OpenData 2.0 data model now supports the License sub-object. In addition, the Licenses can now manage and store multiple IDs from the same issuer using the new dedicated Identifier category. Identifiers are IDs like HIN, NPI, and Tax IDs.

The screenshot shows the profile page for Maricopa Integrated Health Systems. The 'Identifiers' section is active, displaying a table of identifiers. The table has columns for Issuer Name, License/ID Number, Identifier Priority, License Status, and Network ID. There are three active identifiers listed: two NPIs and one HIN. A search bar and a '+ New Identifier' button are also visible.

ISSUER NAME	LICENSE/ID NUMBER	IDENTIFIER PRIORITY	LICENSE STATUS	NETWORK ID
NPI	1987654321	Primary	Active	949308703663785568
NPI	1376643124	Secondary	Active	949345662357538400
HIN	1234567A0	Primary	Active	949341341972760159

The OpenData 2.0 data model, including License support, is enabled by default for new customers. Existing customers can enable the fields for the OpenData 2.0 data model.

Enable License fields for OpenData 2.0

Administrators can enable the fields for their Network MDM instance. The method depends on whether the OpenData 2.0 data model is currently enabled.

OpenData 2.0 not yet enabled

If you have not yet enabled the OpenData 2.0 data model for your Network MDM instance, enabling it will enable all OpenData 2.0 fields for HCPs, HCOs, Addresses, ParentHCOs, and Licenses (including fields for Identifiers).

1. In the Admin console, click **Settings > General Settings**.
2. In the **Common Data Architecture (CDA) and OpenData 2.0 Data Model** section, select **Enable OpenData 2.0 Data Model**.



COMMON DATA ARCHITECTURE (CDA) DATA MODEL AND OPENDATA 2.0 DATA MODEL

☒ Enable Calculations for CDA and OpenData 2.0 [?]
☒ Enable CDA Data Model [?]

☒ **Enable OpenData 2.0 Data Model** [?]

☐ Enable OpenData Identifier Sync [?]

3. **Save** your changes.

OpenData 2.0 data model is already enabled

If you are already using OpenData 2.0, enable the individual License fields.

1. In the Admin console, click **Data Model > Data Domains > Customer Master > Licenses**.
2. In the **Fields** section, expand the Data Schema filter and select **OpenData 2.0**.

All OpenData 2.0 fields display.

3. For any disabled fields, toggle the **Status** icon to **Enabled**.
4. **Save** your changes.

Data Domains > Customer Master > License

License
SUB-OBJECT
On this page: [Object Details](#) · [Fields](#) · [Labels](#) · [Main Objects](#) · [Source Survivorship Rules](#) · [Object Icon](#)

Cancel Save

▼ Fields + Add Field

All countries ▼ All fields ▼ All types ▼ **OpenData 2.0 (30)** ☒ Show disabled fields

Reset Filters

NAME	LABEL	TYPE	REFERENCE TYPE	DATA MODEL SCHEMAS	FIELD ACCESS	STATUS
address_vid_v	Address Network ID	Network ID		OpenData 1.0 OpenData 2.0	All Users	✓ Enabled
best_state_license_v	Best State License?	Checkbox	BooleanReference	OpenData 1.0 OpenData 2.0	All Users	✓ Enabled
collab_agree_required_v	Collaborative Agreement Required	Reference Type	CollabAgree	OpenData 1.0 OpenData 2.0	All Users	⏻ Disabled
comprehensive_prescriptive_authority_v	Comprehensive Prescriptive Authority	Reference Type	ComplLicenseEligibility	OpenData 1.0 OpenData 2.0	All Users	⏻ Disabled
comprehensive_sample_eligibility_v	Comprehensive Sample Eligibility	Reference Type	ComplLicenseEligibility	OpenData 1.0 OpenData 2.0	All Users	⏻ Disabled
country_cda_v	Country (CDA)	Reference Type	AddressCountryCDA	CDA OpenData 2.0	All Users	✓ Enabled

Receive License and Identifier data from OpenData

To learn when License and Identifier data will be available, follow the OpenData communities on Veeva Connect.

- [OpenData - APAC](#) (available by invitation only)
- [Veeva Brazil Commercial Community](#)
- [OpenData - Europe](#)
- [Veeva LatAm Commercial Community](#)
- [OpenData - US](#)



License data

License fields are managed by OpenData by default. Field values are pushed to your Network MDM instance through your OpenData subscriptions or ad hoc downloads as usual.

Identifier data

Important: Veeva OpenData Identifier data is not downloaded to customer instances by default. You must choose to download and sync OpenData Identifier data for your Network MDM instance.

To receive Identifier data from OpenData:

1. In the Admin console, click **Settings > General Settings**.
2. In the **Common Data Architecture (CDA) and OpenData 2.0 Data Model** section, select **Enable OpenData Identifier Sync**.
3. **Save** your changes.

This will set the fields to be OpenData-managed. If this setting is not enabled, Identifiers remain locally managed.

COMMON DATA ARCHITECTURE (CDA) DATA MODEL AND OPENDATA 2.0 DATA MODEL

☒ Enable Calculations for CDA and OpenData 2.0

☒ Enable CDA Data Model

☒ Enable OpenData 2.0 Data Model

☐ Enable OpenData Identifier Sync

Populate field values

After the fields are enabled, follow these steps to populate field values:

1. Enable at least one OpenData 2.0 License field in your Network MDM instance.
2. Run a full OpenData country subscription to update all records that are downloaded in your Network MDM instance.
 - a. Open an OpenData country subscription (**System Interfaces > OpenData Subscriptions**).
 - b. In the **Updates to OpenData records** section, select **Update all records**.
 - c. Save your changes.

The next time the subscription runs, you will receive updates for all the Veeva-managed OpenData 2.0 fields that you have enabled.



License fields

The OpenData 2.0 data model is updated to include the following items for Licenses.

Object	Fields	Reference Types
License	30	20

All fields

To view the complete list of fields that are included, open the **License** object in the Data Model and filter the **Fields** section for all fields that display the OpenData 2.0 data model tag.

New fields

The following new fields are added to the License object. These fields can apply to Licenses and /or Identifiers.

Field Name	Field Label	Field Type	Description	License or Identifier
id_priority__v	Identifier Priority	Reference Type (IdentifierPriority)	Indicates whether the identifier for the HCP or HCO is the primary identifier or an additional (secondary) identifier.	License Identifier
issuer_name__v	Issuer Name	Reference Type (IssuerName)	The official name of the regulatory body, government agency, or professional council that issued the specific license, or the standardized designation of the identifier type assigned to the Health Care Professional or Organization in a certain country.	License Identifier
license_id_number__v	License/ID Number	Text	Unique identifier or license number issued to the HCP/HCO.	License Identifier
license_name__v	License Name	Reference Type (LicenseNameLocal)	License name. Describes what the license is for; for example, Nurse Practitioner.	License Identifier



Field Name	Field Label	Field Type	Description	License or Identifier
object_cat_type__v	Object Category Type	Reference Type (ObjectCategoryType)	This is an important field that determines if the record is a License or an Identifier. Possible values include LICENSE, ID, or no value. Existing Licenses will not have a value. When a record is updated for any reason, the value will be set to LICENSE. Existing Licenses cannot be set to ID. This field is enabled by default for all Network MDM instances.	License Identifier

Existing fields

The following fields have been added to the License object for OpenData 2.0. They apply to Licenses and Identifiers.

Field Name	Field Label	Field Type	Description	License or Identifier
country_cda__v	Country (CDA)	Reference Type (AddressCountryCDA)	Name of country.	License Identifier
entity_object_type__v	Entity Object Type	Reference Type (ObjectEntityType)	Type of the source entity (HCO or HCP).	License Identifier
entity_veevaid__v	Entity Object Veeva ID	Text	Veeva ID of the HCP or HCO associated with this address or license.	License Identifier
license_status__v	License Status	Reference Type (LicenseStatusItems)	License status.	License Identifier
state_cda__v	State/Province (CDA)	Reference Type (AddressStateCDA)	Name of state, province, or regional area.	License Identifier
vid__v	Network ID	Text	Network ID	License Identifier



New reference types

These reference types added for OpenData 2.0 are restricted (read-only); reference codes cannot be added, updated, or removed.

Reference Type	Used by Field	License or Identifier	Details
IdentifierPriority	id_priority__v	Identifier	Two possible values: Primary and Secondary.
IssuerName	issuer_name__v	License Identifier	
LicenseNameLocal	license_name__v	License	
ObjectCateogryType	object_cat_type__v	License Identifier	Two possible values: License and Identifier

To review the reference codes for each new type, go to **Data Model > Reference Data**.

Updates to existing reference types

All reference types for the License sub-object have been updated to be restricted (read-only). Reference codes can no longer be added, updated, or removed from these reference types.

- CollabAgree
- CompLicenseEligibility
- CTRLSubPrescriptive
- CTRLSubSampling
- LicenseCertification
- LicenseDEACode
- LicenseDEAPaymentIndicator
- LicenseEligibility
- LicenseStatusCondition
- LicenseSubType

IDENTIFIERS

26R2

Identifier data is stored on the License sub-object. Identifiers are IDs like HIN and NPI in the US and Tax ID and VAT Number in Europe. Previously, these IDs were stored in record level fields which limited the ability to store more than one type of ID per record; for example, storing multiple NPI numbers on a single HCO record to ensure historical context is preserved during acquisition.

Storing IDs as a sub-object removes these limitations and gives you the flexibility to manage different business scenarios.



Support for Identifier data

Identifiers are introduced with the License sub-object for the OpenData 2.0 data model. They can be stored and managed even if OpenData 2.0 is not enabled for your Network MDM instance.

To use Identifiers:

- Enable the data model fields for Identifiers. See the [License fields](#) section above.
- (Optional) To receive Identifier data from Veeva OpenData, turn on the **Enable OpenData Identifier Sync** option (**Settings > General Settings**).

Defining Identifiers

A new field on the License sub-object, Object Category Type (`object_category_type__v`), determines if the record is a License or an Identifier.

The field is a reference type field that uses the ObjectCategoryType reference list.

ObjectCategoryType reference codes

Network Code	Network Name	Definition	Details
(no value)	-	-	Existing licenses with no value in this field will remain licenses. They cannot be changed to Identifiers. New records with no value will be licenses by default.
ID	Identifier	A unique tracking number assigned to a professional or an organization for administrative or billing purposes, which identifies them but does not grant legal permission to practice.	Identifiers must be explicitly set.
LICENSE	License	A credential granted by a regulatory body that provides legal permission to practice a profession, often with an associated expiration date and status.	This is the default value for new records that do not specify a value for this field.

Impact to existing license records

All existing License records will remain Licenses but they will have no value in the **Object Category Type** field.

When the record is updated for any reason, the (`object_category_type__v`) field will be set to LICENSE. You can also proactively update the field to add the LICENSE value through data loading.

Existing Licenses cannot be changed to Identifiers.



Updating the field

The (object_category_type__v) field cannot be edited after a value is set.

New records

To add an Identifier, the (object_category_type__v) field value must be set to ID.

Add Identifiers in the Network MDM user interface

The (object_category_type__v) field value is determined by the section the record is created in:

- **License section** - The field is set to LICENSE.
- **Identifier section** - The field is set to ID.

Add Identifiers through data loading or the Network API

The (object_category_type__v) field value must be included and set to ID.

If the field has no value or is not defined, the record will be added as a License.

Profile layouts

When the License fields associated with Identifiers are enabled, the **Identifiers** section displays on the GlobalStandard default profile layouts for HCOs and HCPs.

These are the layouts used by the OpenData 2.0 data model.

GlobalStandard (Read Only)
Standard Global Template for HCOs
Created by System
Used by 1 Data Visibility Profile and 0 Widgets

Cancel Clone Delete Save

READ ONLY

General Information

External Identifiers

Licenses

License

Identifier

Identifier

Issuer Name

License/ID Number

Identifier Priority

License Status

Network ID

Custom Fields (License)

Custom Keys

Maricopa Integrated Health Systems

#crm #healthsystem #npi

+1 602-344-1218

FULL ADDRESS 2601 E Roosevelt St Phoenix AZ 85008-4973

Organization, Health System, Unspecified specialty

No value

ID 242976947796182017

Change Record

▼ Identifier (2 active)

Search Identifiers Reset Filters

ISSUER NAME	LICENSE/ID NUMBER	IDENTIFIER PRIORITY	LICENSE STATUS	NETWORK ID
NPI	1987654321	Primary	Active	949308703663785568
HIN	1234567A0	Primary	Active	949341341972760159

Displaying 1 to 2 of 2

Show 10 1 of 1 < >



Fields

The **Identifiers** section includes the following fields:

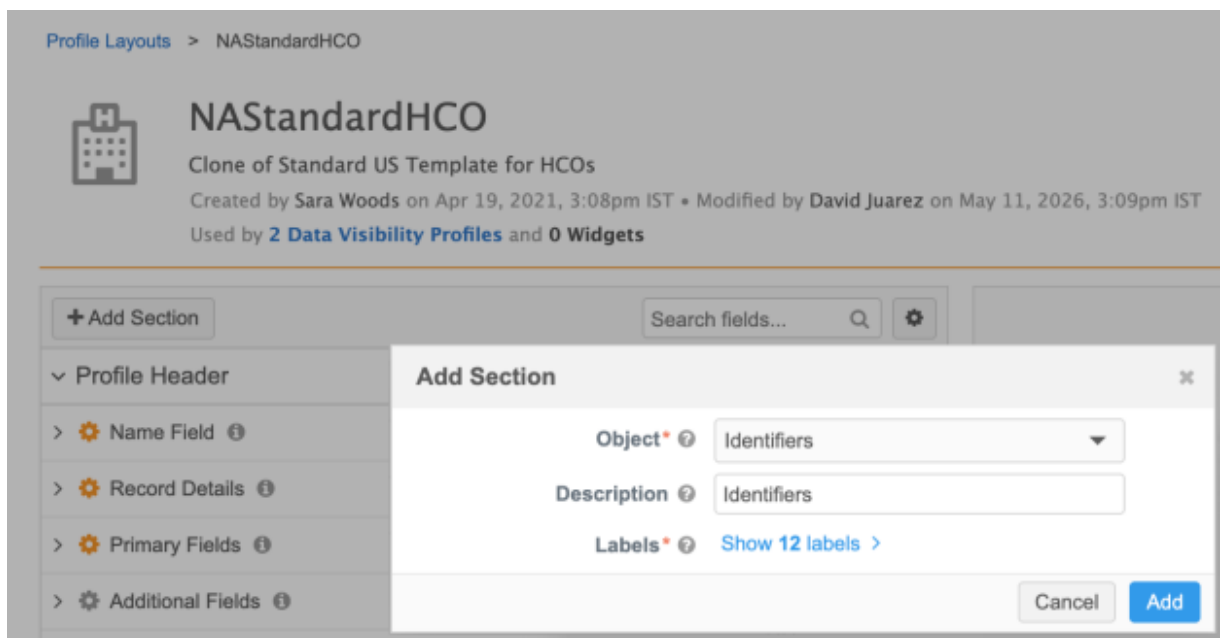
- Issuer Name
- License/ID Number
- Identifier Priority
- License Status
- Network ID

Add to custom layouts

The **Identifiers** section is not added to other standard layouts.

Standard layouts are read-only. Clone a standard layout or edit an existing custom layout to include the **Identifiers** section.

1. In the Admin console, click **Data Model > Profile Layouts**.
2. Choose a custom layout from the list.
3. Click **Add Section**.
4. In the dialog, expand the **Object** field and choose **Identifiers**.
The **Description** and **Labels** fields are automatically populated.
5. Click **Add**.



6. The **Identifiers** section is added to the bottom of the list in the layout. All default fields are included in the section.
Use the **Handle**  icon to move the section to a different location in the layout, for example, below the **Licenses** section.



> Profile Header	
> Primary Information	
> Addresses	
> Parent HCO Affiliations	
> Child Affiliations	
> General Information	
> External Identifiers	
> Licenses	
> Custom Fields	
> Record Information	
▼ Identifiers	

- 7. **Save** your changes.
- 8. If required, update any data visibility profiles (**Users & Permissions**) to use this layout so the **Identifiers** section displays on record profiles.

Identifiers on record profiles

The **Identifiers** section displays on record profiles.

Alta Bates Summit Medical Center Summit South Campus

#hospital

FULL ADDRESS 350 Hawthorne Ave Oakland CA

Organization, Hospital, Multi Specialty Practice

Profile Details

Calls

Primary Information

Addresses

Parent HCO Affiliations

Child Affiliations

General Information

External Identifiers

Licenses

Identifier

▼ Identifier (1 active)

Q Search Identifiers

Reset Filters

+ New Identifier

ISSUER NAME	LICENSE/ID NUMBER	IDENTIFIER PRIORI...	LICENSE STATUS	NETWORK ID	
HIN	123A456BC	Primary	Active	949273291825677920	

Displaying 1 to 1 of 1

Show 10 1 of 1 < >

Supported records

Only License records where the **Object Category Type** field value is ID display in this section.

All other License records display in the **Licenses** section.



Identifier details

The table contains the following details by default:

Column	Description
Issuer Name	The organization that issues the identifier.
License/ID Number	The number issued.
Identifier Priority	The importance of the identifier. Either Primary or Secondary.
License Status	Active or Inactive
Network ID	The 18-character unique ID assigned to the Identifier.
Actions	View custom keys View field details

Available actions

- **Search** - Use the Search bar to find specific identifiers.
- **Sort** - Re-order each column by ascending/descending order.

By default, the table is filtered by the Issuer Name of the Identifier country. If the Country (CDA) field is not included in the profile layout, the Issuer Name is filtered by the primary country of the HCP/HCO record.

- **Reset Filters** - Update the table to the default sorting order.
- **Edit** - Hover over a column value to display the **Edit** icon. Click **Edit** to set the profile page to edit mode.

▼ Identifiers (2 active)					
Search Identifiers		Reset Filters		+ New Identifier	
ISSUER NAME	LICENSE/ID NUMBER		IDENTIFIER Prio...	LICENSE STAT...	NETWORK ID
NPI	1987654321	Edit	Primary	Active	949308703663785568
HIN	1234567A0		Primary	Active	949341341972760159
Displaying 1 to 2 of 2			Show 10 1 of 1 < >		

All Identifier values can be edited except the Network ID.



Adding and updating identifiers

As with all other sub-objects, Identifiers can be updated or added through the Network UI, data loading, and the Network MDM API.

Network UI

Identifiers can be added when you create an HCO or HCP record, or when you edit a record profile.

▼ Identifiers (0 active)

Search Identifiers [Reset Filters](#) [+ New Identifier](#)

COUNTRY (CDA) ⚙	ISSUER NAME ⚙	LICENSE/ID NUMBER ⚙	IDENTIFIER PRIOR... ⚙	LICENSE STAT... ⚙	NETWORK ID ⚙
United State x	No Value	No Value	No Value	Active	178354140167200000 x

Displaying 1 to 1 of 1

Search...
 No Value
 340B
 American Hospital Association
 CMS Certification
 CMS Physician Profile
 DEA
 Group Practice PAC
 HIN
 Massachusetts Covered Recipier
 NCPDP

To add an identifier:

- In the **Identifiers** section, click **New Identifier**.
A row is added to the table.
- Define the following details:
 - Country (CDA)** - The primary country. The primary country of the record profile displays by default.
 - Issuer Name** - The organization that issues the ID.
 - License/ID Number** - The number associated with the ID.
 - Identifier Priority** - The importance of the Identifier: Primary or Secondary.
 - License Status** - Active (default) or Inactive.
 - Network ID** - This is assigned to the Identifier by default.
- Apply** your changes.
The identifier displays in the table.

Note: The **Object Category Type** field value is automatically set to *ID* for objects created in the **Identifiers** section.



Data Loading

Add or update Identifiers using source subscriptions.

Important: Include the **Object Category Type** field with a value of *ID* when loading Identifier data. If the field is not included in the source file, the value is set to *LICENSE* by default. The field value cannot be changed on existing records.

Network MDM API

Submit add requests for Identifiers using the Change Request API.

The Object Category Type (`object_category_type__v`) field must be included in the API call with a value of *ID* to create an Identifier.

There is no impact to existing integrations for creating Licenses; the field does not need to be included because a License is created by default.

Data change requests

When users add or edit an Identifier, a change request is submitted.

DCR routing

The **Enable OpenData Identifier Sync** setting determines where the data change request is routed.

- **On** - Identifiers are managed by OpenData; DCRs are routed to OpenData.
- **Off** - Identifiers are managed locally; DCRs are routed to your local data stewards.

Processing Identifiers on DCRs

An **Identifiers** section is added to add requests and change requests so data stewards can easily process the changes.



Inbox > Change Request - Alta Bates Summit Medical Center Summit South Campus

Change Request

DCR History View CRM Activity Re-assign Reject Save Apply

All Fields **DCR Fields** Collapse All Expand All

Sections: Primary Information · Addresses · Parent HCO Affiliations · General Information · External Identifiers · Custom Keys · Licenses · Custom Fields · Health Care Systems · Additional Fields

Field	Current Value	Change Request	Approved? ▾
▶ Primary Information			
▶ Addresses			
▼ Licenses			
▼ Identifiers			
> IDENTIFIER (NEW)			✓ ✕ ✎
Object Category Type	No Value	Identifier	
License Status	No Value	Active	✓ ✕ ✎
Issuer Name	No Value	HIN	✓ ✕ ✎
Country (CDA)	No Value	United States of America	✓ ✕ ✎
Identifier Priority	No Value	Primary	✓ ✕ ✎
License/ID Number	No Value	123A456BC	✓ ✕ ✎
▶ Additional Fields			

Changes to the Object Category Type field

The **Object Category Type** field cannot be changed after it has been set to *LICENSE* or *ID*. The change will be rejected automatically.

Existing Licenses will have no value for this field. When a record is updated in any way, the field will be set to *LICENSE* by default. Existing Licenses cannot be set to *ID*.



Considerations for other features

Sub-object match rules

Network MDM applies internal sub-object match rules to any merge comparison. The rules use specific fields to compare sub-object records to find duplicates.

To ensure that Licenses and Identifiers are not compared with each other, different fields will be used for each type.

Licenses	Identifiers
license_number__v type_value__v license_degree__v	id__v issuer_name__v

Match configurations

The default match configurations in the Network MDM UI are not updated for Identifiers.

Review your source data to determine if your existing match rules should be updated to prevent over-matching.

Validation rules

Licenses and Identifiers share the same sub-object, so existing validation rules might trigger for both record types.

Review your rules and update them to include the **Object Category Type** field to differentiate between License and Identifier records.

Network Expression (NEX) rules

Review any configured rules and update them to include the **Object Category Type** field to differentiate between License and Identifier records.

Reports

Review your saved reports and update them to include the **Object Category Type** field to differentiate between License and Identifier records.



IQVIA OneKey Connector

The IQVIA OneKey Connector was introduced in Network MDM 26R1.0. The bi-directional connection with IQVIA® OneKey enables you to seamlessly integrate OneKey as your third-party data provider for HCOs and HCPs.

Important: A third-party agreement (TPA) must be in place before OneKey data can be loaded into Veeva Network MDM.

The following enhancements are added in this release.

PROCESSING IQVIA REFERENCE DATA

26R1.1

Network MDM now dynamically manages reference data updates from IQVIA to prevent HCP and HCO record rejections during data loads.

When the IQVIA OneKey source subscription runs, the OneKey custom reference field values in Network MDM (for example, types and specialty) are updated with the list of values from the IQVIA data model. These updates are applied before the data files are processed, eliminating data loading errors caused by missing reference codes.

This enhancement is enabled by default.

OneKey reference data file

As part of the IQVIA OneKey Connector, IQVIA publishes source files to your Network MDM FTP on a regular schedule as delta feeds. One of the files, `codetable.csv`, contains updates to IQVIA reference data.

The file is formatted so it can be consumed by Network MDM and be processed during the source subscription job.

Example file

	A	B	C	D	E	F	G	H	I
1	PROCESS	COUNTRY_LIST	COD_ID_ONEKEY	REFERENCE_TYPE	LIS_LABEL	LIS_CODE	LANGUAGE_CD	COD_SHORT_LBL	COD_LONG_LBL
2	R	"EG,IQ,IO,IB"	DPT_WEG_0040	SubtypeCodeOneKey	Province	DPT	en	Dahok	Dahok
3	R	"FK,GB,IE"	QLF_WUK_3Y	QualificationOneKey	Qualification	QLF	en	Medical Devices	Medical Devices
4	R	"FK,GB,IE"	FAC_WUK_N3	UniversityOneKey	University	FAC	en	Zaire	Zaire
5	R	"AM,AZ,BY,GE,KG,K SD,WRU,R4	EducSpecialtyOneKey	Diploma Specialty	SD	en	en	Child Endocrinology	Child Endocrinology
6	R	"FK,GB,IE"	QLF_WUK_6F	QualificationOneKey	Qualification	QLF	en	Clinical Pharmacology	Clinical Pharmacology
7	R	"CH"	TEN_WCH_1A	TendencyOneKey	Tendency/Medical Interest	TEN	en	Medical examiner	Medical examiner
8	R	"FK,GB,IE"	FAC_WUK_30	UniversityOneKey	University	FAC	en	Burkina Faso	Burkina Faso
9	R	"AM,AZ,BY,GE,KG,K STE,OPE	StateCodeOneKey	State	STE	en	en	Open	Open
10	R	"FK,GB,IE"	DPT_WUK_0017	SubtypeCodeOneKey	County	DPT	en	Greater London	Greater London
11	R	"CH"	SUB_WCH_GEO_C	SubtypeOneKey	Subdivision Level	SUB	de	Geografische Koordinaten	Geografische Koordinaten
12	R	"FK,GB,IE"	FAC_WUK_17	UniversityOneKey	University	FAC	en	Belize	Belize
13	R	"FK,GB,IE"	FAC_WUK_M8	UniversityOneKey	University	FAC	en	West Indies	West Indies
14	R	"EG,IQ,IO,IB"	STE_CLO	StateCodeOneKey	State	STE	en	Closed	Closed
15	R	"EG,IQ,IO,IB"	DPT_WEG_0015	SubtypeCodeOneKey	Province	DPT	en	Ismaileya	Ismaileya
16	R	"FK,GB,IE"	TEN_WUK_L4	TendencyOneKey	Tendency/Medical Interest	TEN	en	Stroke	Stroke



Network MDM uses the following columns to process the IQVIA reference data.

Column	Details
PROCESS	The action. R (Upsert) or D (Delete).
COUNTRY_LIST	The "Active Country" list. The countries listed here determine if the code is added or removed from a country.
COD_ID_ONEKEY	The OneKey reference code.
REFERENCE_TYPE	The custom OneKey reference types used by the IQVIA OneKey connector.
LANGUAGE_CD	The Network MDM language code. IQVIA sends one row for each language. For example, an update for "en" is one row, and an update for "fr" is another row.
COD_LONG_LBL	The translation label for the code description.
COD_END_VAL_DATE	The date the code is valid until on the OneKey side. Typically, the date is defined as 9999-12-31. This date column can be used to inactivate a reference code. Codes are also inactivated using D in the Process column.

The other columns in the file are not considered during the reference data updates.

Supported actions

Changes to the Network MDM reference field values will be made using the following details in the `codetable.csv` file.

Action	Process	Condition
Add reference code for an existing reference type	R	COD_ID_ONEKEY does not exist for the REFERENCE_TYPE.
Add reference codes for active countries	R	COD_ID_ONEKEY exists for the REFERENCE_TYPE and a new country is in the COUNTRY_LIST.
Remove reference codes from active countries	R	COD_ID_ONEKEY exists for the REFERENCE_TYPE and existing country is not in the COUNTRY_LIST.
Create or update reference code translation	R	COD_ID_ONEKEY exists or does not exist, language code is defined in LANGUAGE_CD, and COD_LONG_LBL is populated.
Inactivate reference codes	D	COD_ID_ONEKEY exists for the REFERENCE_TYPE.
Inactivate reference codes	R	COD_ID_ONEKEY exists and COD_END_VAL_DATE is different from 999-12-31.



Reference update job

When your IQVIA OneKey source subscription runs, the reference data job runs first as a separate job. The `codetable.csv` file is loaded and processed before the data files (`hcp.csv`, `hco.csv`) are loaded.

The job displays in the **Job History** section.

Job History							
1 of 106 < >							
View Job Impact Dashboard							
ID	START TIME	DURATION	PROCESSED HCOS	PROCESSED HCPS	RUN TYPE	OUTCOME	JOB TRIGGERS?
639	2026-05-26 15:09:46 IST	a minute	165	2,011	BY JOB	COMPLETED	No
638	2026-05-26 15:09:46 IST	a minute	479	2,740	BY JOB	COMPLETED	No
637	2026-05-26 15:09:46 IST	a minute	250	3,813	BY JOB	COMPLETED	No
636	2026-05-26 15:09:46 IST	a minute	114	1,325	BY JOB	COMPLETED	No
635	2026-05-26 15:09:45 IST	a minute	0	0	BY JOB	COMPLETED	No

Click the **Job ID** to open the Job Details page.

On the page, you can see that the `codetable.csv` file was processed. Job statistics are not currently available for the reference data updates.

Job Details (ID: 635)

[View Job Impact Dashboard](#)
[Cancel Job](#)

Job Summary

Job Error Log

Overview

System

IQVIA-OneKey

Subscription

IQVIA_OneKey

Start Time

2026-05-26 15:09:45 IST

End Time

2026-05-26 15:10:37 IST

Job ID

635

Duration

a minute

Percent Complete

100.00%

Current Stage

FinalStage

Outcome

COMPLETED with errors and warnings

Started By

PM Admin

Number of Files Processed

1

Number of Bad Records

2

Job Settings Summary

Files Loaded Summary

Network FTP Path

Inbound/IQVIA/OneKey/GCC

Folder / ZIP File

GCC

ALIAS

REFERENCE

FILE NAME

codetable.csv

Data Load Summary

Processed Data Summary

ENTITY

RECORDS PROCESSED

Health Care Organization

0

Health Care Professional

0



The relevant fields in the `codetable.csv` file are validated. If any required field is empty, the invalid row is dropped and a warning displays on the **Job Error Log** tab.

Job Details (ID: 635) [View Job Impact Dashboard](#) [Cancel Job](#)

Job Summary **Job Error Log**

[Download Job Error Log](#)

ERROR CODE	MAIN OBJECT	MAIN OBJECT ROW NUMBER	ERROR MESSAGE	SEVERITY
E0027	All Codes ✕	All Items ✕	DCR processing was skipped. No DCR response file(s) found - originating... more	Error
W0063	codetable.csv	6	Invalid reference data: missing reference type at line 6	Warning

Displaying 1 to 2 of 2 Show 10 1 of 1 < >

The job continues so the OneKey HCP and HCO data updates can be processed.

Warnings

The following warnings are created for IQVIA reference data issues.

Code	Details	Action
W0063	A row is missing a value for the mandatory REFERENCE_TYPE column, making it impossible to categorize the record.	Populate the REFERENCE_TYPE field for the specified line in your source file to ensure the code is mapped to the correct category.
W0064	The unique identifier for a reference code (COD_ID_ONEKEY) is missing for the specified reference type.	Provide the missing code value in the source file. Every reference entry must have a unique ID to be processed by Network MDM.
W0065	The mandatory PROCESS column (instruction) is empty, so the system does not know whether to add/update or delete the code.	Add the appropriate instruction to the PROCESS column (for example, R for Replace/Update or D for Delete).
W0066	The value provided in the PROCESS column is not supported. Only R (Replace) and D (Delete) are recognized.	Correct the instruction value in the source file to either R or D as required.
W0067	The reference code entry is missing a language code (LANGUAGE_CD) for its label.	Ensure a valid ISO language code (for example, "en", "fr") is provided in the LANGUAGE_CD column for the specified line.
W0068	The language code provided in the LANGUAGE_CD column is not supported or recognized by the system.	Verify and correct the language code to a supported standard format. Ensure the language is supported in Network MDM.
W0069	The mandatory start date for the reference code's validity (COD_BEG_VAL_DATE) is missing.	Populate the COD_BEG_VAL_DATE column in your source file with a valid start date.



Code	Details	Action
W0070	The value provided for the begin-valid date is not a recognized date format (YYYY-MM-DD).	Correct the date in the COD_BEG_VAL_DATE column to match the expected format (YYYY-MM-DD).
W0071	The reference code entry is missing an end-valid date (COD_END_VAL_DATE).	Provide a valid end date in the source file. For codes that do not expire, use a far-future date or the standard system default.
W0072	The value provided for the end-valid date is incorrectly formatted or contains invalid characters.	Verify and correct the date format in the COD_END_VAL_DATE column of your source file.
W0073	The descriptive label for the reference code (COD_LONG_LBL) is missing.	Provide a descriptive label in the COD_LONG_LBL column to ensure the reference code is identifiable in the UI.
W0074	Multiple rows for the same reference code were found with contradictory instructions (for example, one row says Delete, another says Replace).	Review the source file for duplicate entries of the same reference code. Ensure the PROCESS instruction is consistent across all rows for that code.
W0076	The mandatory country list for the reference code's validity (COUNTRY_LIST) is missing.	Populate the COUNTRY_LIST column in your source file with a valid list of countries.

Simulation mode

If the source subscription job is run in Simulation Mode, the reference data updates in the `codetable.csv` file will be processed. The data updates will remain simulated as usual.



UNMERGE ONEKEY RECORDS

26R1.1

Network MDM can now process unmerges that are sent from IQVIA in a source file. When your IQVIA OneKey source subscription runs, the OneKey records are unmerged. Previously, source subscription jobs processed the merged records only.

This enhancement is enabled by default.

Unmerged records file

IQVIA publishes OneKey source files to your Network MDM FTP as scheduled delta feeds. One of the files, **merge_unmerge_events.csv**, contains merges and unmerges that need to be actioned in your instance.

The records IQVIA has merged and unmerged are identified by the OneKey ID value. When the source subscription runs, Network MDM will now unmerge the records in your instance.

Example merge_unmerge_events file

merge_unmerge_events.csv								
343 Rows No Filters Applied								
PROCESS	CHILD_ENTITY_TYPE	CHILD_ID_ONEKEY	PARENT_ID_ONEKEY	PARENT_ENTITY_TYPE	LINKTYPE_CODE	BEG_VAL_DATE	END_VAL_DATE	ACTION_TYPE
R	W	WUSE00235302	WUSE00006259	W	ENTITIES_LINK_WUS_DOU	2011-05-11	9999-12-31	M
R	W	WUSE00442157	WUSH00001488	W	ENTITIES_LINK_WUS_DOU	2019-04-04	9999-12-31	M
R	W	WUSE00439640	WUSH00001488	W	ENTITIES_LINK_WUS_DOU	2019-04-04	9999-12-31	U
R	W	WUSE00375182	WUSH00072691	W	ENTITIES_LINK_WUS_DOU	2019-04-04	9999-12-31	M
R	W	WUSE00751505	WUSE00166344	W	ENTITIES_LINK_WUS_DOU	2018-06-08	9999-12-31	M
R	W	WUSE00015232	WUSH00003920	W	ENTITIES_LINK_WUS_DOU	2019-04-04	9999-12-31	M
R	W	WUSE00602055	WUSE00001176	W	ENTITIES_LINK_WUS_DOU	2019-04-04	9999-12-31	M
R	W	WUSE00407929	WUSH00002990	W	ENTITIES_LINK_WUS_DOU	2011-03-30	9999-12-31	M
R	W	WUSE00659807	WUSH00003920	W	ENTITIES_LINK_WUS_DOU	2018-04-03	9999-12-31	U

The file contains the following important fields:

Column	Details
PROCESS	Instructions on how to handle the data: R (Upsert) or D (Delete)
CHILD_ENTITY_TYPE	The object type of the losing record: W (Workplace (HCO)) or I (Individual (HCP)).
CHILD_ID_ONEKEY	The OneKey ID of the losing record (the new unmerged record).
PARENT_ID_TYPE	The OneKey ID of the of the winning record.
PARENT_ENTITY_TYPE	The object type of the winning record: W (Workplace (HCO)) or I (Individual (HCP)).
ACTION_TYPE	The action taken: M (Merge) or U (Unmerge).

The other columns in the file are not considered during the unmerge action.



About the unmerge job process

Source subscriptions will unmerge the records identified by IQVIA before processing the updates in the data files. This ensures merged records are successfully split and isolated first, preventing the incoming data feed updates from updating the winning merge record with data from the losing record.

Unmerged records

When the records are unmerged, the following actions are taken for each record.

Winning record

- Any active custom keys belonging to the split record are inactivated.

Split record (new unmerged record)

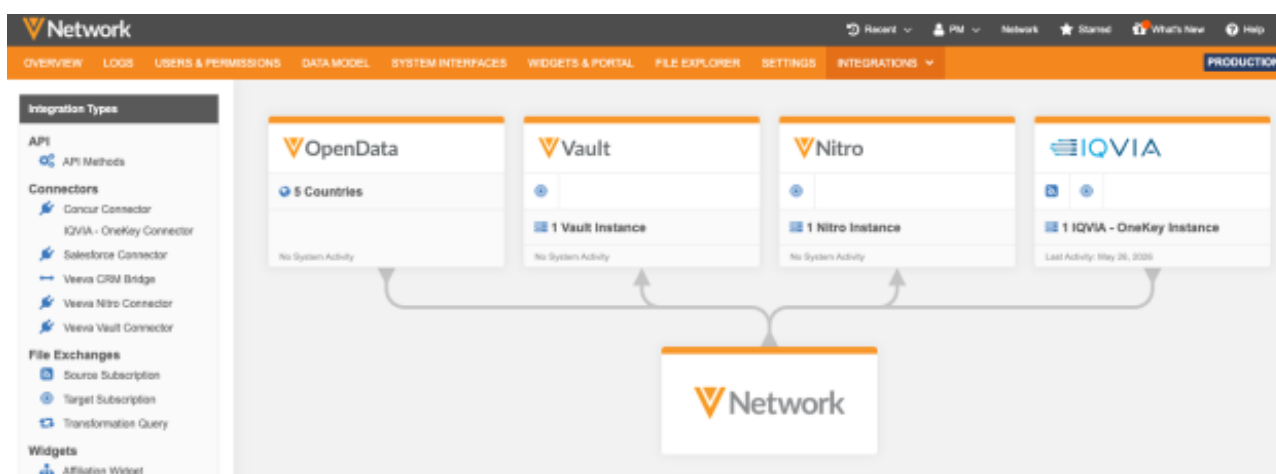
- A new Network ID is assigned.
- IQVIA custom keys originally associated with the record before it was merged are returned to the record.

Important Customer-owned sub-objects and fields cannot be moved to the new record. You must add them back to the new unmerged record. Use reporting to help identify the sub-objects and fields to bring back.

INTEGRATION DASHBOARD

26R1.1

The IQVIA - OneKey Connector is now included in the high-level system summary on the Integration Dashboard. Administrators can click the IQVIA system to view the specific configuration details.



This enhancement is enabled by default if you have an IQVIA OneKey system configured in your Network MDM instance.



IQVIA OneKey configurations

From the dashboard, click the system to open the configuration pop-up.

System Details

The **Details** tab displays by default. It contains the IQVIA-OneKey system configuration

System: IQVIA-OneKey

Details

Name IQVIA-OneKey

Type IQVIA - OneKey

Icon

Dataflow Type BI-Directional

Description

Third Party Master Yes

Unmerge ability Do not unmerge

[Save Details](#)

Integration details

Click on an integration to view more details. For example, click **Source Subscriptions** to see details about the job that loads the IQVIA OneKey data. The time of the last job displays in your timezone.

- Click the subscription name to navigate to that subscription configuration.
- Click the link in the **Last Job Status** column to open the job details for the latest job.



System: IQVIA-OneKey-DEV

Details

Source Subscriptions

Target Subscriptions

Search Source Subscriptions

NAME	LAST RUN	SCHEDULE	LAST JOB STATUS
IQVIA_OneKey	2026-05-26 15:10:36 IST	Manual	COMPLETE



Data model

NEW FIELDS FOR UNMERGED RECORDS

26R2

To make record history clearer and easily to track, three new fields are added to unmerged records to provide the following information:

- Record that the new (unmerged) record was unmerged from.
- Original record that the data is being restored from.
- Date of the unmerge.

The screenshot displays a patient profile for John Jacobson. The profile includes a header with the patient's name, a star icon, and a list of roles: #Emergency, #md, #npi, and #physician. Below this, the full address, HCP type (Prescriber), and primary specialty (Emergency Medicine) are listed. On the right, contact information (email, phone, and ID) is provided. The main content area is divided into sections: Primary Information, Addresses (1 active), E-Contacts, Educational Information, and Record Information. The Record Information section is expanded, showing fields for Created Date, Modified Date, Status Modified Date, Unmerged Date, Unmerged From Network ID, and Unmerged Original Record Network IDs. The Unmerged Date, Unmerged From Network ID, and Unmerged Original Record Network IDs fields are highlighted with orange boxes. The Unmerged Original Record Network IDs field contains a long string of IDs: 949307889902813223;949307889902944283. On the right side of the profile, there is a Hierarchy section showing a tree structure with William Fisher at the top, and a Revision History section showing two entries: Update from change request (2026-07-15 EDT) and Add from Unmerge (2026-07-15 EDT).

This enhancement is enabled by default. The fields are enabled by default in all instances.

Benefits

- **Easily cleanup bad merges** - Bad merges can occur from broad matching rules, bad source files, data stewardship, and overmatching in jobs. These fields provide the exact pre-merge IDs you need to understand the record's history.
- **Track all unmerge activity**: Automatically audits any unmerge action, whether it was triggered by Veeva OpenData or local data stewards.
- **Simpler downstream data updates** - Downstream systems can read these fields directly, removing the need to build custom code to detect when records are unmerged.

Note: Existing unmerged records will not be backfilled.



New fields

The following system fields are enabled by default and cannot be disabled. They are managed by Veeva OpenData by default.

Field Name	Label	Description
record_unmerged_date__v	Unmerged Date	Date when the record was unmerged
record_unmerged_from_vid__v	Unmerged from Network ID	Network ID of record that this record was unmerged from
record_unmerged_original_vids__v	Original Record Network IDs	The Network IDs of the records that existed before they were merged. It confirms which original record's data is now being restored into the new record. Note: The Unmerged From Network ID field value will never be included in this field.

Supported records

The fields are available on main objects only.

- HCP
- HCO
- custom main objects (including Payers and Plans)

About unmerged records

Unmerging records is an existing process in your Network MDM instance and in Veeva OpenData. Records are typically unmerged due to overmatching or to separate records that were manually matched in error. This enhancement adds details to an unmerged record, making it easy to instantly see the history of the original record and the record it was separated from.



Example scenario

- **The Merge:** Record A and B are merged into Record C. Record C now contains the combined data lineage of both original records.
- **The Unmerge:** Record B is unmerged from C.
- **The Result:** A new record, B1, is created.

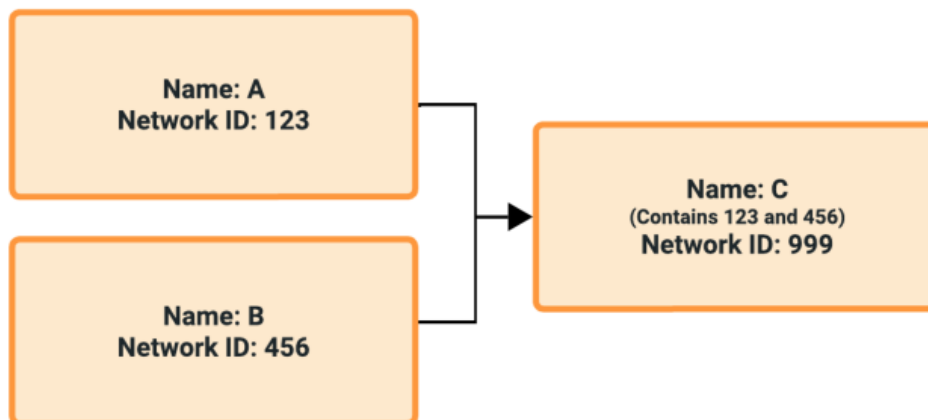
The new fields are added to B1 to give you full visibility into the history of the record:

- The Network ID of the merged record it came from (Record C).
- The Network ID of the original record (Record B).

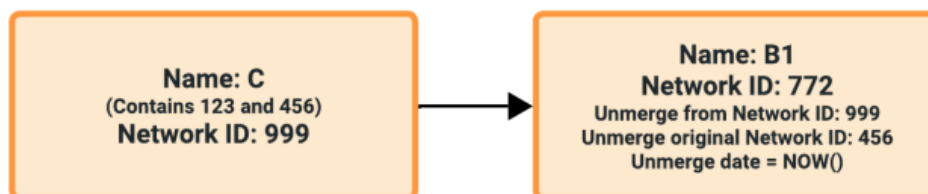
This tells you the source of the bad merge and identifies where the data for B1 originates. If there are multiple Network IDs, they are always sorted in ascending order and are separated by double-semi-colons (;).

- The unmerge date.

Merge A and B into C



Unmerge B from C





View the fields on record profiles

The fields are added to the **Record Information** section on standard profile layouts by default.

Add the fields to any custom profile layouts that you've created for HCPs, HCOs, and custom objects.

Cholecap 5mg ☆

ENTITY TYPE Product
NETWORK ID 949311695587704865

Primary Information

Record Information
External Identifiers
Indications
Parent Market Baskets
Packages
Brands

Record Information

Created Date	2026-07-16 10:42:45	Modified Date	2026-07-16 10:42:45
Status Modified Date	2026-07-16 10:42:45	Surviving Record Network ID	No Value
Unmerged Date	2026-07-16 10:42:45	Unmerged From Network ID	949311681457684511
Unmerged Original Record Network IDs 949311685285969951			
Product Type		Regulatory Identifier	

Unmerged fields on OpenData records

The new fields are available on OpenData records that are downloaded to your Network MDM instance. This gives you more transparency on unmerges that occur on OpenData records.

Note: The Network IDs of the original or unmerged from record might not be in your instance or be available to download.



Report on unmerges

Advanced reporting users can report on unmerges using the sample queries available in the SQL Query Editor (**Reports**).

Example sample query - Unmerged HCPs

The screenshot shows the SQL Query Editor interface. The query is a UNION of two SELECT statements. The first SELECT statement filters for HCPs, and the second filters for HCOs. Both statements select fields: vid__v AS "New VID", record_unmerged_from_vid__v AS "Unmerged From", record_unmerged_original_vids__v AS "Unmerge Original VIDs", 'HCP' AS "Entity Type" (or 'HCO' for the second statement), record_owner_type__v AS "Source", and record_unmerged_date__v AS "Unmerged Date". The WHERE clause for both is record_unmerged_from_vid__v IS NOT NULL.

Below the query editor, a status bar indicates "Query Valid" and a checkbox for "Include only VALID and UNDER_REVIEW records in results." is checked.

The "Report Results (2 records)" section displays a table with the following data:

NEW VID	UNMERGED FROM	UNMERGE ORIGINAL VIDS	ENTITY TYPE	SOURCE	UNMERGED DATE
949308320808239146	949307889902747681	949307889902813223;949307889902944293	HCP	OpenData	2026-07-16 00:24:30
949312210635784223	949307889902551079	949307889902682161;949307889902878773	HCP	OpenData	2026-07-16 16:53:44

At the bottom, it says "Displaying 1 to 2 of 2" and "Show 25" with pagination controls.

New unmerge queries

New sample queries are available which include the new unmerge fields. They report on unmerges in your Network MDM instance and in the OpenData instance.

- Unmerged HCOs
- Unmerged HCPs
- Unmerged HCPs and HCOs

Existing unmerge queries

The names of the existing sample queries for unmerged HCPs and HCOs are updated to indicate that they are legacy reports. These queries report on unmerges that occurred in your Network MDM instance only.

- Unmerged HCOs (Legacy)
- Unmerged HCPs (Legacy)
- Unmerged HCPs and HCOs (Legacy)



CLUSTER MANAGEMENT

26R1.1

Updated cluster codes are available for the following country/third-party cluster provider combinations:

Cluster Provider	Country	New Version
IQVIA	Spain	6.0
IQVIA	United Kingdom	4.0

The new cluster version is available by default if you have the country/provider combination enabled in your Network MDM instance.

Update addresses

To update addresses with the latest cluster codes:

1. In the Admin console, click **Data Model > Cluster Management**.
2. Select the country / IQVIA cluster configuration.
3. In the **Cluster Management Details** section, expand the **Cluster Version** field and choose the latest version.
4. **Save** your changes.
5. Click **Refresh Addresses** to run a data maintenance job to ensure that all addresses for that country have the latest cluster codes.



OpenData subscriptions

ADVANCED FILTERS

26R2

Administrators and Data Managers now have greater flexibility for defining which records to include in a country subscription. Using SQL queries, you can create advanced filters to specify additional records for download.

You can also now view any Veeva-managed filters currently applied to your instance directly within the subscription settings.

The screenshot displays the 'Veeva OpenData Subscription (France)' configuration page. At the top right, there are buttons for 'Cancel', 'Ad Hoc Download', 'Start Job', and 'Save'. Below the title, three radio buttons are present: 'No additional records', 'Additional records via Basic Filters', and 'Additional records via Advanced Filters' (which is selected). Under the 'Advanced Filters' section, there is a 'Query Description' field containing the text 'Doctors specializing in Oncology'. Below this is a 'Query' section with a text area containing an SQL query:

```
1 SELECT
2   vid__v
3 FROM
4   opendata_emea.hcp
5 WHERE
6   hcp_type__v = 'D'
7   AND specialties = 'ON'
8   AND primary_country__v = 'FR'
```

 To the left of the query text are line numbers 1 through 8. Above the query text are buttons for 'Format Query' and 'Copy to Clipboard'. Below the query text is a green checkmark icon and the text 'Query Valid'. At the bottom of the form, there is a 'Preview Additional Records' button and a field labeled 'Additional Records to be Added' which displays the number '2865'.

This enhancement will be enabled by default for your Network MDM instance.



Filter options

When your OpenData country subscription runs, it downloads and updates records defined in your working set file. Previously, you could filter by Specialty and Type in the UI or submit a Veeva Support ticket for custom filtering.

With this release, you can now build advanced filters using SQL queries directly in the UI, giving you greater control over which HCP and HCO records are downloaded.

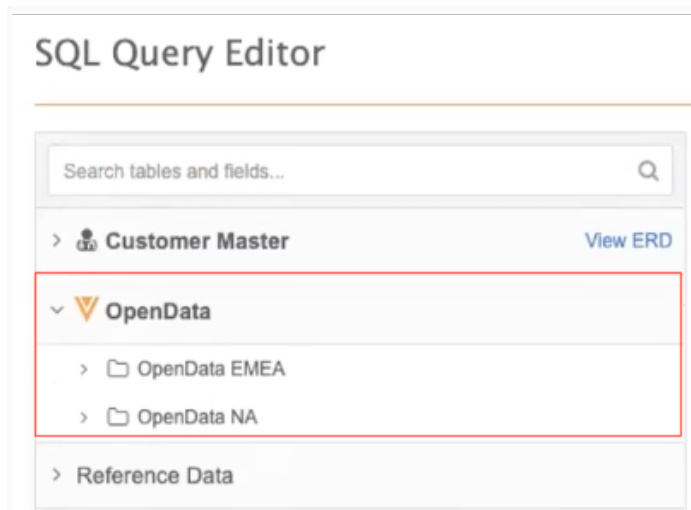
The HCP and HCO section in country subscriptions now have the following filter options.

Filter Option	Details
No additional records	Subscribe to records in the Working Set file only. (default)
Additional records via Basic Filters	Filter records by Specialty or Type.
Additional records via Advanced Filters	Use SQL queries to subscribe to additional records. These queries are defined and tested in the SQL Query Editor using the OpenData reporting tables and then copied and used in your OpenData country subscriptions. Queries run in your instance against OpenData reporting tables.
Additional records via Managed filters	Queries are created and managed by Veeva. The queries display as read-only so you can easily understand what is currently in place. In some cases, you can convert a Managed filter to an Advanced Filter that you can self-manage.

Create an advanced filter

Prerequisite

The Reporting on OpenData feature must be enabled in your Network MDM instance. The queries are created using fields from the OpenData tables. If the feature is enabled, the **OpenData** category displays in the SQL Query Editor.



For more information about this feature, see [Reporting on OpenData](#) in the *Veeva Network MDM Online Help*.

Process

- Write and test query in the SQL Query Editor.
- Copy and paste the query to the country subscription and preview the count of additional records that will be subscribed to using the filter.

Add an advanced filter:

1. Open the SQL Query editor (**Reports**) and define a query using the OpenData reporting tables.

Queries must filter on a primary country and include a SELECT statement, a WHERE clause, and reference the OpenData master instance tables.

See the [Query validation](#) section for additional requirements and restrictions.

Example query

Use this HCP query to subscribe doctors in France that specialize in Oncology.

```
SELECT
    vid__v
FROM
    opendata_emea.hcp
WHERE
    hcp_type__v = 'D'
    AND specialties = 'ON'
    AND primary_country__v = 'FR'
```

The query will validate as you create it.



Sample Queries My Recent Queries Query Helper: Keywords Operators Format Query

```

1 SELECT
2     vid__v
3 FROM
4     opendata_emea.hcp
5 WHERE
6     hcp_type__v = 'D'
7     AND specialties = 'ON'
8     AND primary_country__v = 'FR'
9

```

Query Valid ☒ Include only VALID and UNDER_REVIEW records in results. ⓘ

Report Results (2,866 records) Download Report Create Custom Table View Full Screen

NETWORK ID

560995918984250382
560995922222253084
560995938001224708
560995961942311974
560995972000252929

- Click **Run Query** to test the query and get a count of all OpenData records that meet your filter criteria.
- Open the OpenData country subscription (**System Interfaces > OpenData Subscriptions**).
- In the **HCP** or **HCO** section, click **Additional records via Advanced Filters**.
- Type a **Query Description**.
- Paste the validated query into the **Query** box.

The query will validate again.



Veeva OpenData Subscription (France) Cancel Ad Hoc Download Start Job Save

☐ No additional records
☐ Additional records via **Basic Filters**
☒ Additional records via **Advanced Filters**

Query Description
Doctors specializing in Oncology

Query
Format Query Copy to Clipboard

```
1 SELECT
2   vid__v
3 FROM
4   opendata_emea.hcp
5 WHERE
6   hcp_type__v = 'D'
7   AND specialties = 'ON'
8   AND primary_country__v = 'FR'
```

Query Valid

Preview Additional Records

Additional Records to be Added
2865

7. Click **Preview Additional Records**. A count displays the number of additional records that will be added to your subscription. This is calculated by taking the records in OpenData that match the filter and subtracting any you already have in your instance.
8. **Save** your query.
9. In the **Save Changes** dialog, the option **When this subscription runs, download all OpenData records that meet the defined criteria** is selected by default. Click **Yes, Save Changes**.

Save Changes ✕

HCP/HCO filters have been modified.

☒ When this subscription runs, download all OpenData records that meet the defined criteria.

No Yes, Save Changes



Query validation

All queries must include a SELECT statement and be complete and valid.

In addition, the following rules are applied to ensure the queries are valid.

Validation Rule	Validation Message	Details
Network ID (vid__v) must be from the HCP or HCO OpenData table that you are querying	Invalid Selection: The query must select only the vid__v field from the HCP or HCO table. Please remove any additional fields or aliases.	Only Network IDs are added to subscriptions.
Use available reporting tables	Unknown Table: Only OpenData tables as well as custom or lookup tables can be queried.	Any referenced tables must be one of the following: - OpenData master instance table ('opendata_<region>.hcp' or 'opendata_<region>.hco') - custom table in your instance (includes __ct suffix) - lookup table in your instance (includes __t suffix)
Include a WHERE clause	Missing Filter Criteria: A WHERE clause is required. Please add specific filter criteria to your query.	-
Cannot include a DISTINCT keyword	Unsupported Clause: The DISTINCT keyword is not allowed. Records are unique by default within the OpenData subscription.	-
Cannot include a LIMIT clause	Unsupported Clause: The LIMIT clause is not allowed in this context. Please use the WHERE clause to manage the scope of your results.	-
Cannot include a MIN, MAX, COUNT, and so on	-	Aggregate functions are not supported. The query supports only the vid__v field from the HCP or HCO table.



Managed filters

If you have existing filters that were requested through Veeva Support tickets, the **Additional records via Managed Filters** option displays. The query created and managed by Veeva displays as read-only so you can see what is currently in place to subscribe to additional records.

Veeva OpenData Subscription (Austria) Cancel Ad Hoc Download Start Job Save

Health Care Professional Subscribe to additional HCP records in addition to any HCP VIDs listed in the Working Set file.

☐ No additional records

☐ Additional records via **Basic Filters**

☐ Additional records via **Advanced Filters**

☒ Additional records via **Managed Filters** ⓘ

Filters are currently managed by Veeva OpenData (Zendesk 607732, 1440439, 1461157). Switch to 'Advanced Filter' to customize your filter configuration.

Format Query Copy to Clipboard

```
1 SELECT
2   DISTINCT h.vid__v
3 FROM
4   hcp h,
5   parent_hco p,
6   hco o
7 WHERE
8   h.hcp_status__v = 'A'
9   AND h.vid__v = p.entity_vid__v
10  AND p.parent_hco_status__v = 'A'
11  AND o.hco_status__v = 'A'
12  AND o.vid__v = p.parent_hco_vid__v
13  AND h.candidate_record__v = 'N'
14  AND o.candidate_record__v = 'N'
15  AND ( h.data_privacy_opt_out__v IS NULL OR h.data_privacy_opt_out__v = 'N')
16  AND h.primary_country__v IN ('AT')
17
18  AND r
```

Switch to an advanced filter

You can remove the Managed filter and create an Advanced filter so you can manage it for your instance.

Options

- Write a new query
- Copy the Managed filter and use it as starting point for your Advanced filter.

Important considerations

Because Advanced filters run against OpenData reporting tables in your Network MDM instance—rather than on the OpenData instance—existing Veeva-managed queries cannot simply be copied; they must be adjusted or rewritten.



Example issues

- **Custom tables and custom fields** - If the Managed filter uses Veeva custom tables or custom fields, the filter behavior must be changed because you cannot access those Veeva artifacts.

Contact your OpenData representative before converting a Managed filter that uses Veeva tables or custom fields.

- **Candidate record fields** - References to candidate record fields must be removed. They are not included in OpenData reporting tables.
- **Include the OpenData tables** - The FROM statement must include the OpenData instance table for the entity; for example, `opendata_emea.hcp`.

The query must be fully tested in the SQL Query Editor before being added as an Advanced filter.

Create the advanced filter

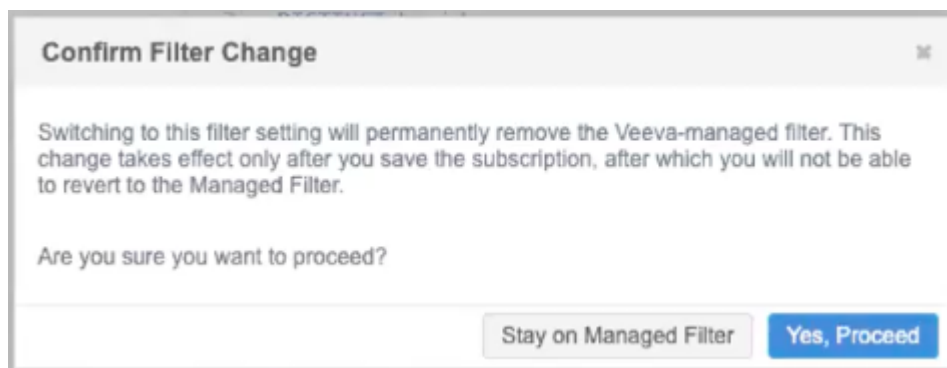
Important: The switch from a Managed filter to an Advanced filter cannot be reversed.

To switch from using a Managed filter to an Advanced filter:

1. If you are copying the Managed filter, click **Copy to Clipboard**.
2. Open the SQL Query Editor (**Reports**) and either paste the copied Managed filter query and make the required changes or create a new query.

Ensure that the query validates and then run it to view the results.

3. Copy the query and open the OpenData country subscription.
4. Select **Additional Records via Advanced Filters**.
5. In the dialog, confirm that you want to switch to using an advanced filter. Click **Yes, Proceed**.



The **Additional records via Managed Filters** option is removed.

6. In the **Additional records via Advanced Filters** option, type a **Query Description**.
7. Paste your tested query. When the query validates, click **Preview Additional Records** to test the query against the OpenData reporting tables. A count displays the records that will be added to your country subscription.
8. **Save** your changes.



UPDATES FOR FIELD MANAGEMENT

26R2

OpenData country subscription settings are updated with clearer field labels, making it easier for Administrators and Data Managers to understand and select which fields are managed by OpenData.

The following improvements have been made to the **Fields** section:

- **Labels** - The labels for each pane are updated to indicate field management.

Previous Label	New Label
Available Fields	Managed by Customer
Selected Fields	Managed by OpenData

- **Field names** - The field name now displays beside each field label, for example, # of Beds (count_beds__v).

The screenshot displays the 'Veeva OpenData Subscription (United States)' interface. At the top, there are buttons for 'Cancel', 'Ad Hoc Download', 'Start Job', and 'Save'. Below the title, a section titled 'Veeva OpenData Fields' contains a descriptive paragraph: 'Select fields for which you wish to receive OpenData in this country. OpenData will begin populating the data in those fields. Migrate any existing customer owned data presently loaded into those fields prior to enabling.' The interface is divided into two main panes. The left pane, titled 'MANAGED BY CUSTOMER', contains a search bar and a list of categories: 'HCO', 'Parent HCO', 'HCP', 'Address', and 'License'. The right pane, titled 'MANAGED BY OPENDATA', also has a search bar and a list of specific fields under the 'HCO' category. These fields include: '# of Beds (count_beds__v)', '# of Inpatients (count_inpatients__v)', '# of MDs and DOs (count_md_do__v)', '# of MDs and DOs all locations ...', '# of Medical Staff (count_medstaff__v)', '# of Medical Staff all locations ...', '# of Outpatients (count_outpatients__v)', '# of non-MDs and DOs (count_non_md_do__v)', '# of non-MDs and DOs all locations ...', and '% of Medicaid Patients (percent_medicaid__v)'. The field label '# of Beds (count_beds__v)' is highlighted with a red box. Navigation arrows are located between the two panes.

These enhancements are enabled by default.

ENHANCED JOB DETAILS

26R2

The **Job Result Summary** now includes a new column called **Processed** to display the total count of processed records. Previously, this data was available only in the **Job History** section on the country configuration.

This update provides immediate clarity on the full scope of a job, making it easy to see exactly how many records the job evaluated compared to how many actually resulted in a change.

In addition to the new column, a header clearly separates the count of records processed during the job versus the updates that were made.

Veeva OpenData Subscriptions > Veeva OpenData Subscriptions (United States) > Job Details (ID: 4444)

Job Details (ID: 4444) [View Job Impact Dashboard](#) [Cancel](#)

► Overview

▼ Job Result Summary [View Job Impact Dashboard](#)

ENTITY	PROCESSED	CHANGES MADE IN THIS INSTANCE							
	TOTAL	TOTAL	ADDED	CANDIDATES ADDED	UPDATED	MERGED	INVALIDATED	NOT LOADED	REJECTED
Health Care Organization	4,577	1,149	506	0	643	0	0	0	0
Health Care Professional	1,202	903	20	203	2	0	0	0	0
License	4,928	787	738	0	73	0	0	0	0
Parent HCO	9,012	2,202	1,213	0	781	0	0	0	0
Custom Key	9,570	9,120	5,330	0	4,240	0	0	0	0

This enhancement is enabled by default.

Processed records

Processed records are the records included in the exported files when the OpenData subscription ran. This could be a full export (scheduled to run every Sunday from each OpenData instance) or a delta export (scheduled to run at least once a day from each OpenData instance) which contains records that were updated since the last export.

The columns in the **Changes Made in This Instance** section display counts for any record that meets one of these three criteria when a job runs:

- If there are updates for a record that has already been downloaded, it makes those updates.
- If there are records that meet any filters for a particular country, those records are downloaded.
- If new Network IDs were added to the Working Set file and those ID are in the exported files from OpenData, those records are downloaded.



PRIMARY CDA ADDRESS FIELD

26R1.1

The Primary CDA field (`primary_cda__v`) for the Address object can now be managed by Veeva OpenData. Previously, the field could be locally managed only.

This change is available by default. Administrators can change the field ownership within their OpenData country subscriptions.

Data impact

Leave as locally managed (default behavior)

There is no data impact if the `primary_cda__v` field remains locally managed.

Change to OpenData managed

If you choose to make the field managed by OpenData for a country, the following behavior occurs:

- Data change requests will be routed to OpenData data stewards for processing
- Updates to the field will be provided through your OpenData country subscription.
- Locally managed data in the field will be overwritten by OpenData data.

Tip: Backup existing data in the field before receiving updates from OpenData. See [Tips for preserving local data](#) in the *Veeva Network MDM Online Help*.

Update the field

To change the field to be mastered by Veeva OpenData:

1. In the Admin console, click **System Interfaces > Veeva OpenData Subscriptions**.
2. Open a country subscription.
3. In the **Veeva OpenData Fields** section, expand the **Address** section in the **Managed By Customer** pane.
4. Select the **Primary (CDA)** (`primary_cda__v`) field and use the **Right-Arrow** icon to move it to the **Managed by OpenData** pane.



▼ Veeva OpenData Fields

Select fields for which you wish to receive OpenData in this country. OpenData will begin populating the data in those fields. Migrate any existing customer owned data presently loaded into those fields prior to enabling.

MANAGED BY CUSTOMER

Search fields

▶ HCO

▶ Parent HCO

▶ HCP

▼ Address

Billing (billing_cda__v)

Home (home_cda__v)

OneKey ID (onekey_id__v)

OneKey ID of Owner (entity_onekey_id__v)

Primary (CDA) (primary_cda__v)

Sample Shipping (sample_shipping_cda__v)

Shipping (shipping_cda__v)

MANAGED BY OPENDATA

Search fields

▼ HCO

of Beds (count_beds__v)

of Inpatients (count_inpatients__v)

of MDs and DOs (count_md_do__v)

of MDs and DOs all locations ...

of Medical Staff (count_medstaff__v)

of Medical Staff all locations ...

of Outpatients (count_outpatients__v)

of non-MDs and DOs (count_non_md_do__v)

of non-MDs and DOs all locations ...

% of Medicaid Patients (percent_medicaid__v)

»

>

<

«

5. **Save** your changes.
- The field will now be managed by OpenData for that country.
6. Repeat these steps for each country where OpenData will manage the field.



Subscriptions

COUNTRY VISIBILITY FOR JOBS

26R2

Country information is now available for the Job History and on the Job Details page so Administrators and Data Managers can instantly see which countries are impacted by each job run.

For global teams with subscriptions that trigger multiple country-specific jobs, this change simplifies monitoring, speeds up troubleshooting, and makes it easy to verify exactly where data updates and exports are being applied.

ID	START TIME	DURATION	COUNTRIES	PROCESSED AFFILIATIONS	PROCESSED HCOS	PROCESSED HCPS	OTHER PROCESSED RECORDS	RUN TYPE	OUTCOME	JOB TRIGGERS?
39697	2026-07-07 13:09:52 EDT			0	0	100	0	MANUAL	✓ COMPLETED	No
39043	2026-06-24 10:20:45 EDT			0	0	100	0	MANUAL	✓ COMPLETED	No
39042	2026-06-24 10:18:52 EDT	a minute	19 countries	0	0	100	0	MANUAL	✓ COMPLETED	No
39040	2026-06-24 10:12:36 EDT	a few seconds	United States	0	0	100	0	MANUAL	✓ COMPLETED	No
39039	2026-06-24 10:11:27 EDT	a few seconds	United States	0	0	100	0	MANUAL	✓ COMPLETED	No

This enhancement is enabled by default in your Network MDM instance.

Supported jobs

- Source Subscriptions
- Target Subscriptions
- OpenData Subscriptions
- Data Updater
- All other jobs except Veeva Connector and Network Bridge jobs

Country details

Country information displays in the Job History section and on the Job Details page. Depending on the job type, these are the countries where records were loaded or exported by the job.

- **Job History** - A **Countries** column is added to this section on subscription configurations.
- **Job Details** - A **Countries** field is added to the Overview section.



Job Details (ID: 40172)

Cancel Job

Job Summary

Job Error Log ⓘ

▼ Overview

System

BBM

Subscription

export_hcps

Start Time

2026-07-18 04:25:07 EDT

End Time

2026-07-22 16:02:16 EDT

Job ID

40172

Duration

a few seconds

Percent Complete

100.00%

Current Stage

FinalStage

Outcome

✔ COMPLETED

Countries

United Kingdom, Zimbabwe, United States

Type

Data

Started By

System

Full Data Extract

Yes

Delta Tag Start

0

Delta Tag End

949215288775704575

Level of Hierarchy Exported

1

Country details

The country is defined by the `primary_country__v` field on the record.

Display

- **Five countries or less** - The country name and flag displays If there are more than five countries, a count displays.
- **More than five countries** - A count of countries displays as a link. Click the link to open a pop-up that contains the list of countries.

Countries

✕

COUNTRIES (19)

Trinidad & Tobago

Germany

Andorra

Belgium

India

Japan

South Africa

Italy

Mexico

You can also hover over the count to see the list of countries.



- **No countries** - N/A displays for jobs that ran before this release. Previous jobs are not back-filled with country information.

N/A also displays for source subscription jobs that ended before the merge stage of the job.

Job History										
View Job Impact Dashboard										
ID	START TIME	DURATION	COUNTRIES	PROCESSED AFFILIATIONS	PROCESSED HCOS	PROCESSED HCPS	OTHER PROCESSED RECORDS	RUN TYPE	OUTCOME	JOB TRIGGERS?
39038	2026-06-24 10:10:31 EDT	a few seconds	N/A	0	0	100	0	MANUAL	COMPLETED	No

Source subscriptions

ADVANCED PROPERTIES FOR REFERENCE DATA UPDATES

26R1.1

Administrators can configure source subscriptions to allow records to be processed even when reference data is missing or inactive for a target country. This ensures that reference data issues do not block you from getting high-priority data updates (like address or name changes). You can also define the fields that must fail when reference data is missing.

The following advanced properties can be added to the Source Subscription configuration (**Advanced Mode**):

Advanced Property	Value
<code>"job.merge.ignore.invalid.referenceData": "true/false"</code>	- true - Enables the partial update behavior. The record will be updated but you will see a warning in the Job Error Log about the reference data issue so you can fix it. - false (default) - Retains current behavior of rejecting the record.
<code>"job.merge.disallow.invalid.referenceData.for.fields": "<field>,<field>,"</code>	A comma-separated list of field names from any object that must reject the record for bad reference values if validation fails (for example, <code>primary_country__v</code> or <code>specialty_1__v</code>). This property is ignored if the above property is false.

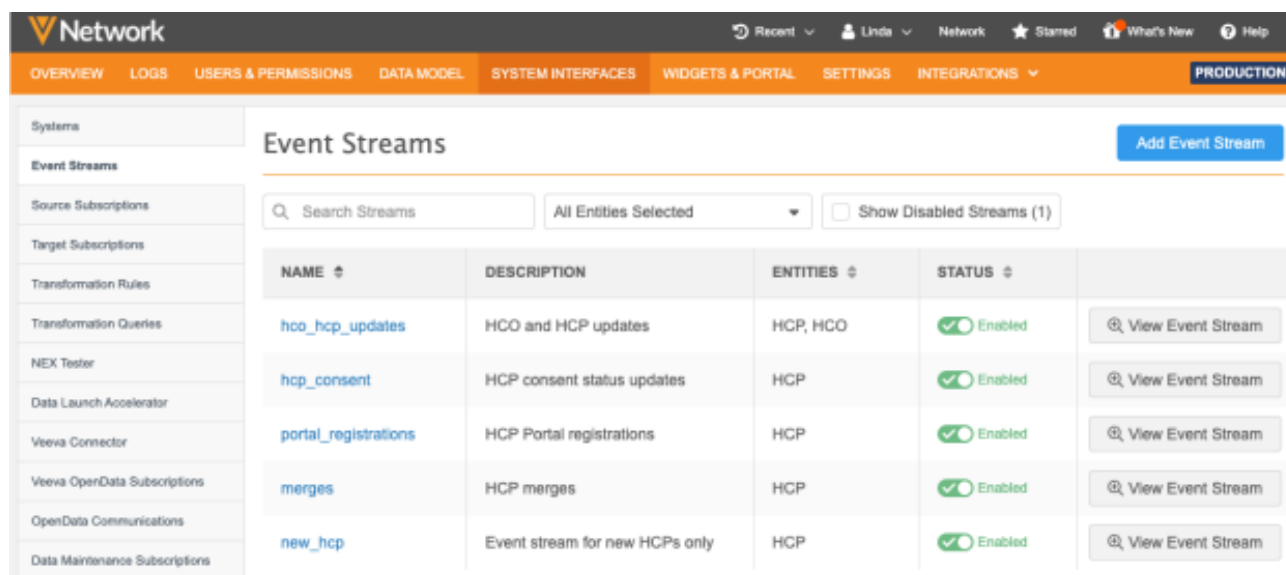
This enhancement is available by default. Administrators can set the properties in the subscription configuration.

Integrations

EVENT STREAMS

26R2

Event Streams is a new integration pattern that you can use to immediately notify downstream systems about time and business critical updates.



NAME	DESCRIPTION	ENTITIES	STATUS	
hco_hcp_updates	HCO and HCP updates	HCP, HCO	Enabled	View Event Stream
hcp_consent	HCP consent status updates	HCP	Enabled	View Event Stream
portal_registrations	HCP Portal registrations	HCP	Enabled	View Event Stream
merges	HCP merges	HCP	Enabled	View Event Stream
new_hcp	Event stream for new HCPs only	HCP	Enabled	View Event Stream

This feature will be available by default in your Network MDM instance for the 26R2.0.1 Production release (August 21, 2026).

Benefits

- **Real-time updates** - Data reaches downstream systems much faster than scheduled exports.
- **Efficiency** - Eliminates the need for repetitive full-data exports.
- **Precision** - Uses filters and triggers to capture only the exact data required for your specific requirements.

Comparison of export patterns

To accommodate diverse export requirements, Network MDM supports multiple export options. In addition to traditional scheduled file exports and request/response API calls, the Event Stream feature allows downstream systems to consume specific data changes in near real-time.

Network Export Feature	Method	Data Format
Target subscriptions	Scheduled or manual delta/full exports to Network MDM FTP or external Amazon S3 bucket.	CSV
API	Custom clients submit requests to Network MDM API endpoints and then based on that request; a response is sent in real-time.	JSON (Request/Response)



Network Export Feature	Method	Data Format
Event Stream	Real-time push of specific changes to a named stream using Apache Kafka. Custom consumers connect to the stream and read the messages sent into the stream.	JSON (Messages)

How event streams work

This feature uses an Apache Kafka® infrastructure to operate on a Producer-Consumer model to notify your downstream systems.

- **The Producer** (Network MDM) - Monitors for specific data updates (new and changed records) based on your event stream configuration. When a change meets the criteria, a message is generated.
- **Event Stream** - A message queue ("Kafka topic") that persists these messages in JSON format.
- **The Consumer** - A custom-built application on the customer-side (can, for example, be a simple Python script or a consumer configured through a middleware). It authenticates to Network MDM's Apache Kafka broker, connects to a specific event stream, and then reads the messages.

For details about event streaming, see the [Apache Kafka Online Help](#).

Supported changes

Adds and updates to records through change requests and data loading will be included in event stream messages.

Note: You can configure each event stream to filter the adds and updates that are included in the messages.

Getting started

The process to configure an event stream consists of the following tasks.

Network MDM configuration

- **Create an Integration User** - The user that authenticates to the Kafka broker to read the event stream messages.
- **Define an event stream** - Define the data changes that will trigger a message to be created.

External configuration

- **Develop the Consumer** - Build your integration client to connect and authenticate to Network MDM's Kafka broker and read from a specific event stream.



Create an Integration user

Add an Integration user for accessing event streams.

Note: Existing Integration Users that have FTP and/or API access cannot also access event streams. This new Integration User must access event streams only.

1. In the Admin console, click **Users & Permissions > Users**.
2. Click **Add User**.
3. Type a **Username**.
4. Type the user's **Email** address.
5. Expand the **User type** list and select **Integration User**.
6. In the **Contact Information** section, add the user's **First Name** and **Last Name**.
7. Choose **Generate temporary password and notify user**. The user will receive a Welcome email from Network MDM with a link to change their password
8. In the **Additional Permissions** section, change the **Event Stream Access** setting to **Allow**.

▼ **Additional Permissions**

API Access	Don't Allow ▼
FTP Access	Don't Allow ▼
Event Stream Access	Allow ▼
Metadata Access	Limited By Data Visibility Profile ▼

Note: The **API Access** and **FTP Access** settings are now dimmed. They cannot be set to **Allow** if the **Event Stream Access** is **Allow**.

9. **Save** your changes.
10. Below the **Event Stream Access** setting, the **Generate Security Token** button now displays. Click the button to view the token.

▼ **Additional Permissions**

API Access	Don't Allow ▼
FTP Access	Don't Allow ▼
Event Stream Access	Allow ▼
	<button>Generate Security Token</button>
Metadata Access	Limited By Data Visibility Profile ▼



Copy the token and store it securely until it is used in the consumer configuration. It will be used with the Integration User's username to authenticate to Network MDM's Kafka broker.

The dialog box titled "Generate Security Token" contains the following text: "The event stream security token has been generated successfully. It is shown below and **will only be displayed once**. Please copy and store it securely." and "Use this token in combination with the integration username to authenticate against the Network MDM Kafka Broker." Below this, it says "Security Token:" followed by a text field containing the token "LZUEJxdEi0dEKYrQuIwhxDN0QHUUwLRqGNgnYxC". At the bottom right, there are two buttons: "Copy Token to Clipboard" and "Done".

Important: The token displays only once. You can generate a new token at any time if needed.

11. Click **Done**. The security token is now masked.

The "Additional Permissions" panel shows several settings: "API Access" set to "Don't Allow", "FTP Access" set to "Don't Allow", "Event Stream Access" set to "Allow", "Security Token in Use" showing a masked token ".....gnYxC" with a "Reset Security Token" button next to it, and "Metadata Access" set to "Limited By Data Visibility Profile".

If required, use the **Reset Security Token** button to generate a new token.

Define an event stream

This configuration defines the entities, types of changes (adds, updates), and optional field conditions that will trigger a message to be created and pushed to your downstream system.

1. In the Admin console, click **System Interfaces > Event Streams**.
2. Click **Add Event Stream**.

Note: A limit of 20 active event streams can be created. When the maximum number is reached, the **Add Event Stream** button is dimmed.



3. Details section:

- **Name** - Type a name.
Supported characters: lowercase letters, numbers, underscores ('_').
- **Description** - Create a meaningful description.
- **System** - Select the source system for the event stream.

The data in the message queue contains reference aliases that are tied to the system.

4. **Event Stream Access** - Add the Integration Users that will access the event stream from your Kafka consumer.

- **Broker URL** - This URL will be used in your consumer connection settings. It is generated by Network MDM.

Naming convention: <POD_name>-streams.veevanetwork.com:<port_number>

Example: vdm21-streams.veevanetwork.com:9196

- **Users** - Click **Add Users** to choose the users that will access this event stream.

The dialog displays Integration Users with the **Event Stream Access** permission.

NAME	USERNAME	USER TYPE	STATUS	SECURITY POLICY
Smith, John	john.smith@verteo.veevanetwork.com	Integration User	Active	Basic



5. **Entity Filters** - Define the entities to include in the event stream.

- **Entity** - For example, choose **HCP**.

Optional filters can be added to define specific entities.

For example, to limit the event stream only to HCPs in the US, define the following filter:

- **Field** - The field to filter on. (*Primary Country*)
- **Condition** - The criteria the filter must meet. (*Equals*)
- **Value** - Select or type the value. (*United States*).

FIELD	CONDITION	VALUE	AND/OR
HCP Primary Country X	Equals	United States	X

+ Add Field

Click **Add Entity Filter** to add another filter for a different entity.

6. **Event Triggers** (*Optional*) - Define specific changes to the entity that will send a message into the event stream.

Important: If triggers are not defined, all adds and updates for the entity will send a message to the event stream.

- **Entity** - Choose the entity.
The main entity and all sub-objects and relationship objects display in the list.
- **Action** - Choose which type of change will trigger a message:
 - **New record is added**
 - **Existing record is changed**
- **Add Condition** - Define specific changes that will trigger a message.
 - **Field** - Choose the field.
 - **Old Value** - Choose the condition for the previous field value. (Displays only when the **Action** is set to **Existing record is changed**).
 - **New Value** - Choose the condition for the updated value.

Additional conditions are OR operations.



Example - Changes to HCP consent status

To update your downstream system immediately when there are changes to HCP consent, define the following triggers:

Event Trigger	Setting	Value
Trigger 1		
	Entity	HCP - Consent
	Action	Existing record is changed
	Condition	Field - Consent Status Old Value - Is Changed
Trigger 2		
	Entity	HCP - Consent
	Action	New record is added

These conditions will limit the messages in the event stream to changes to HCP consent status.

Event Triggers

Define the specific changes to the entities selected above that will trigger a message into the event stream.

Entity
HCP - Consent

Action
Existing record is changed

CONDITION

Field
Consent Status

Old Value
Is Changed

New Value
Select Option

+ Add Condition

OR

Entity
HCP - Consent

Action
New record is added

CONDITION

Optional: If no conditions are defined, any records with the selected action on the selected entity will trigger a message, regardless of field values.

+ Add Condition



7. **Field Selection** - Define the fields to be included in the event stream messages.

By default, all fields are included in the message. These are the same fields that are included when the entity is retrieved in the API. You can exclude fields from the message if they should not be consumed by your downstream system.

8. **Save** your changes.

Preview the event stream

After the event stream is created, validate that it is correctly configured to include the messages that you've defined.

- On the Event Stream page, click **View Event Stream**.

The dialog will display the 20 most recent messages. To see messages display, change or add records to meet the filters/trigger conditions in your stream.

For each message, the following details display:

- **Created At** - The date of the revision.
- **Entity VID** - The Network ID of the entity.
- **Revision Number** - The revision number of the update. This is the same revision number that displays on the Profile page for the record.
- **Action** - The type of change: Add, Update, or Merge.



View Event Stream: hcp_consent

Find the most recent messages added to the event stream below:

Refresh

CREATED AT	ENTITY VID	REVISION NUMBER	ACTION
2026-04-22 07:18:08 EDT	946933665358217260	4.0	UPDATE
<pre>{ "consent_set__c": [], "parent_hcos__v": [] }, "changes": [{ "metadata": { "vid__v": "946933665358217260", "revisionId": "2309598814406969344", "revisionNumber": "4.0", "revisionType": "VALUES_AND_METADATA", "createdAt": "2026-04-22T11:18:08.524Z", "verb": "Update" }, "gender__v": { "previousValue": null, "previousSource": null, "updatedAt": "F", "updatedSource": "change_request" }, "primary_country__v": { "previousValue": "US", "previousSource": "customer", "updatedAt": "US", "updatedSource": "change_request" } }] }</pre>			
2026-04-21 03:56:16 EDT	948823138430681119	2.0	UPDATE
2026-04-21 03:56:14 EDT	948823138430681119	1.0	ADD

View the message

Expand the row to view the actual message that will be sent to your downstream system.

- **Entity details** - The first part of the message contains the entity details. These are the same details that are included, for example, in a retrieve call on an entity from the API.

Only the entities that you defined in the **Filters** section of the event stream generate messages into the stream.

- **Revision details** - The revisions details display in the **changes** section of the message.
 - Revision metadata - Network ID, revision ID, number, and type; date of the change; and the action.

Note: If the source that made the change is different from the previous source, the **revisionType** parameter identifies that change also. The parameter value will be **VALUES_AND_METADATA**.

- Field revisions - The changes for each field: previous value and updated value.

The event stream is now ready. Messages can be received by the consumer.



Develop the consumer

A Kafka consumer must be implemented to retrieve the messages that Network MDM sends into the event stream.

A *Consumer* reads messages from the stream and processes them for downstream systems. This ensures the downstream system can process data at its own pace.

For details, see the [Apache Kafka consumer Configs](#) documentation.

Consumer process

The consumer establishes a secure session to the Network MDM Kafka broker and connects to the specific event stream. It reads the messages, processes them, and manages the so-called "offset". The *offset* is like a bookmark that tells the consumer what message to start reading from the next time it connects. This ensures that there is no data duplication or loss between connections.

Requirements

To build the consumer, you need the following details from your Network MDM Administrator.

Parameter	Details	Example
Kafka Broker	The Kafka Broker URL and port number. The URL generated by Network MDM to connect to the event stream. Copy and paste the complete broker URL, including the port number, from the Event Stream configuration.	KAFKA_BROKER = vdm21-streams.veevanetwork.com:9196
Kafka Topic	The topic that you want to consume messages from. This is the name of the event stream in Network MDM that is prefixed with your Network MDM instance ID. Find your Network MDM ID in Settings > General Settings .	KAFKA_TOPIC = '11043.new_hcps'
group.id	Your consumer group ID. This consumer group ID must be prefixed with your Network MDM instance ID.	'group.id': '11043.my_consumer_group',



Parameter	Details	Example
auto.offset.reset	Where you want to start consuming messages if no previous offset is found. The value can be one of the following: - earliest - Start reading from the oldest available message in the topic. - latest - Ignore messages sitting in the Kafka topic and start reading from the end of the queue.	'auto.offset.reset': 'earliest',
security.protocol	Use SASL over SSL for secure communication. Use these values: 'security.protocol': 'SASL_SSL', 'sasl.mechanisms': 'SCRAM-SHA-512',	
sasl.username	The integration user that has access to the event stream. This user must have the Event Stream Access permission set to <i>Allow</i>.	'sasl.username': 'john.smith@verteo.veevanetwork.com',
sasl.password	The security token generated by Network MDM for the Integration user. The token is used to authenticate against the Kafka broker. Copy the token from the Integration User profile. If the token is masked and cannot be copied, reset the token.	'sasl.password': 'tDudyhRKWQeWVZLtnUHqGT YjgiJQkvfCiqUUUNSk',
enable.auto.commit	The option for manually or automatically committing offsets. Values can be <i>True</i> or <i>False</i>.	'enable.auto.commit': False

Offset management

In Kafka, every message has a unique ID called *Offset*. Each consumer identifies itself to the Kafka broker through the Consumer Group ID ('group.id'). Multiple consumers can be grouped to share the workload of consuming the messages. Each consumer group uses the offset to know where to continue picking up messages.

Message retention

All messages in the event stream are kept for four weeks by default. The offset ensures that the consumer doesn't read all messages each time it connects to the event stream. It also ensures that messages are not missed when your Network MDM instance or your consumer client are experiencing a downtime.



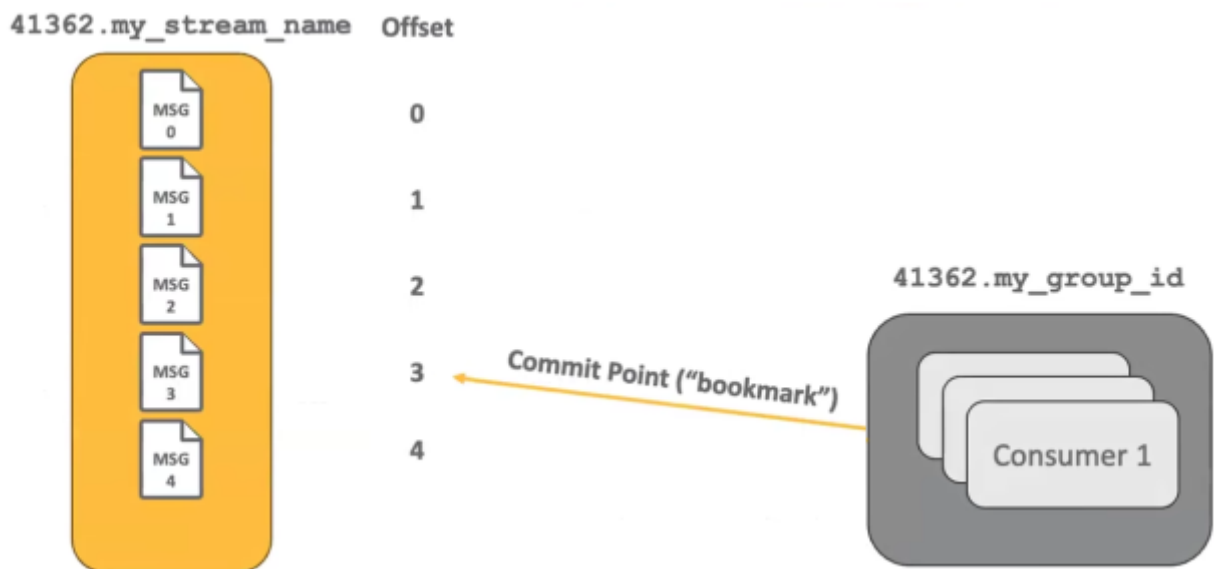
Commit points ('enable.auto.commit')

The commit point is a bookmark strategy that the consumer uses to tell the Kafka broker that it is done consuming the messages.

- **'enable.auto.commit' = 'true'** - The consumer automatically tells Kafka every few seconds that it is done with the messages.
- **'enable.auto.commit' = 'false'** - The consumer must explicitly tell Kafka that it is done with the messages.

Commit point example

In this example, the commit point is at message 3. This means that messages from 0-3 have been read by the consumer. The next time the Kafka broker or consumer restarts, the consumer will begin reading messages from message 4.



Offset reset ('auto.offset.reset')

The reset tells Kafka where the consumer will start reading after re-starting the consumer.

- **'auto.offset.reset' = 'earliest'** - Start reading from the oldest message in the event stream.
- **'auto.offset.reset' = 'latest'** - Start reading from the first new message in the event stream.

Using the commit point example above, when the consumer restarts, *earliest* resets your bookmark to message 0 again, while *latest* skips ahead to start reading from message 4.



Avoid duplicating data across streams

Only create different streams if they provide different data to the downstream systems. Do not create event streams that generate the same messages for the same entities.

Example

If you have the following event streams defined, each revision on an HCP/HCO will generate two messages.

- **Event Stream 1** - Export all HCPs and HCOs
- **Event Stream 2** - Export all HCOs
- **Event Stream 3** - Export all HCPs

Exporting duplicate data multiplies the data being persisted in the event streams in your Network MDM instance and degrades performance.

Considerations for multiple consumers

If you have several consumers that need to read similar data, they should share the same event stream.

To do this, assign different Integration users to the same event stream or use different consumer group IDs.

Turn off an event stream

When an event stream is no longer needed, Administrators should disable it on the Event Streams page or in the configuration. No further messages will be sent to the stream. This is especially recommended for event streams that were created for testing purposes in sandbox instances.

Enable the event stream again

If the event stream is re-activated, messages will resume flowing into the stream again. New messages are generated from the point in time when the stream was enabled again. Events that occurred while the stream was off cannot be retrieved.

Sandbox instances

After an event stream has been tested in your Sandbox, turn it off to prevent the data from flowing unnecessarily.



VAULT CRM CREDENTIAL

26R2

To simplify integrations, Vault CRM provisions a dedicated Network System User in each Vault CRM instance. This enhancement allows Vault CRM administrators to manage the Network MDM integration without maintaining a Vault Integration username and password. This single-purpose user eliminates conflicts with other integrations that use the same user and removes issues that can occur when passwords expire.

To support this change, in your Network MDM instance, you can now create a secure connection to Vault CRM using the new Vault CRM credential type. Previously, the Vault credential was used with the Vault Integration user and password.

This feature is enabled by default in your Network MDM instance.

About the Network System User in Vault CRM

A Network System User is provisioned in Vault CRM for every Vault CRM instance. This user replaces the Vault Integration user. The user is set with predefined permissions, but you will need to extend the permissions for the user to be fully functional. For example, provide access to object types and custom fields.

The Network System User will be supported in [Vault CRM 26R2.0 \(August 2026\)](#).

New Vault CRM implementations

When you are setting up a new Vault CRM implementation, the Network System User is enabled by default on the Network Integration Administration page (**Configuration**).

The **Credentials** section displays the **Vault URL** and the **User**. The naming convention of the user is `application-network_int@<vault_domain>`.

Example

The screenshot shows the 'Vault CRM' interface. The top navigation bar includes 'Admin', 'Logs', 'Users & Groups', 'Configuration' (selected), 'Operations', 'Deployment', 'Connections', 'Settings', and 'About'. The left sidebar has 'COMPONENTS', 'RECENTLY USED', and 'FAVORITES'. The main content area is titled 'Network Integration Administration' and contains two sections: 'Network Credentials' and 'Vault Credentials'. The 'Vault Credentials' section is highlighted with a pink box and shows the following details:

Vault URL	User
vertio.veevavault.com	application-network_int@vertio.veevavault.com

Note: In the **Network Credentials** section, add the Network URL and Network Integration User as usual so you can connect your Network MDM instance to Vault CRM.



Existing Vault CRM implementations

If you are already integrating with Vault CRM, update your Vault CRM and Network MDM configurations to use the Network System User.

Important: After switching to the Network System User, the change cannot be reversed.

Process

The following tasks must be completed in Vault CRM and Network MDM to update the integration to use the Network System User.

- **Vault CRM** - Complete the prerequisite tasks for the Network System User.
- **Network MDM** - Create a Vault CRM credential. This new credential type uses the Network System User to connect Network MDM to Vault CRM.
- **Network MDM** - Update the Vault CRM Bridge to use the new Vault CRM credential.
- **Vault CRM** - Switch from using the Vault Integration user to the Network System User.

Prerequisite tasks for the Network System User

Complete these tasks in Vault CRM:

- Update the permissions for the Network System User based on your business needs. For example, provide access to custom fields and object types.
- Create or update Veeva Settings and Network Settings for the Network System User Application Profile (**System User Application Profile**).
- Create a Veeva Support ticket to update data change requests that are pending from Vault CRM to include the Network System User.

Create a Vault CRM credential

Add a Vault CRM credential in your Network MDM instance. This new credential type uses the Network System User instead of the Vault Integration user.

Supported features

The new credential can be used for the following features:

- Data Launch Accelerator
- Vault CRM Bridge
- Validate Vault CRM Bridge

Note: The Vault CRM credential is not supported for Veeva Connectors and Vault Data Components. Continue using a Vault credential for these features.

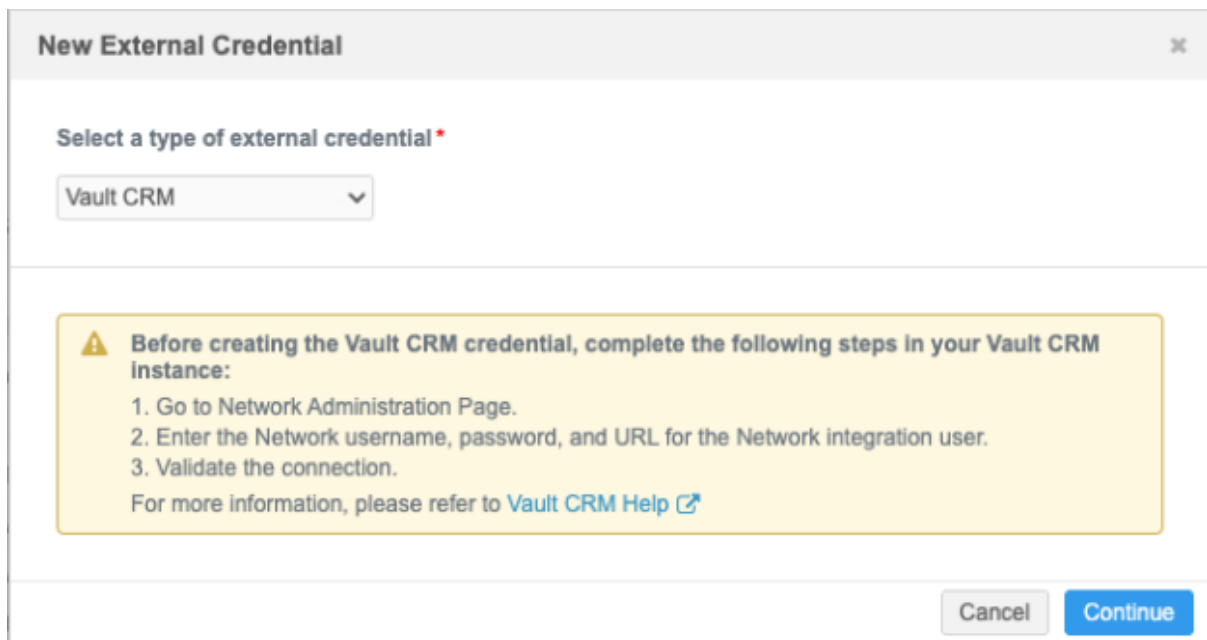


Add the credential

1. In the Admin console, click **Settings > External Credentials**.
2. Expand the list and choose **Vault CRM**.

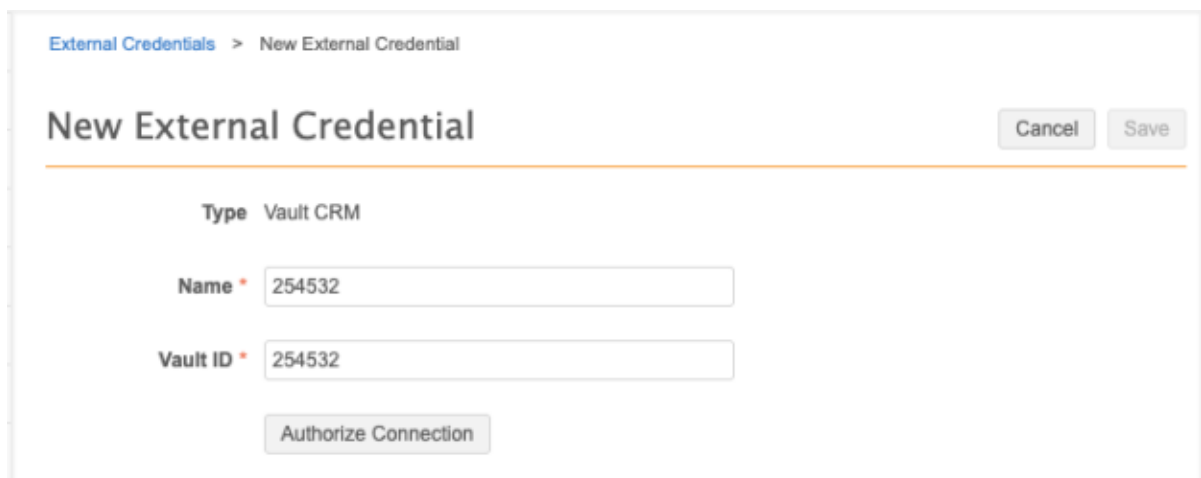
Review the information in the dialog and ensure that the Network Integration username, password, and URL are added to the Network Administration page and that the connection is valid.

For details, see [Administrative Tools](#) in the *Vault CRM Online Help*.



The dialog box is titled "New External Credential" and has a close button (X) in the top right corner. It contains a section "Select a type of external credential *" with a dropdown menu showing "Vault CRM". Below this is a yellow warning box with a triangle icon, containing the text: "Before creating the Vault CRM credential, complete the following steps in your Vault CRM instance: 1. Go to Network Administration Page. 2. Enter the Network username, password, and URL for the Network integration user. 3. Validate the connection. For more information, please refer to [Vault CRM Help](#)". At the bottom right are "Cancel" and "Continue" buttons.

3. Define the Vault CRM credential **Name**.
4. Type the **Vault ID**.



The form is titled "New External Credential" and has a breadcrumb "External Credentials > New External Credential". It has "Cancel" and "Save" buttons in the top right. The form shows "Type" as "Vault CRM". Below are two required fields: "Name *" with the value "254532" and "Vault ID *" with the value "254532". At the bottom is an "Authorize Connection" button.

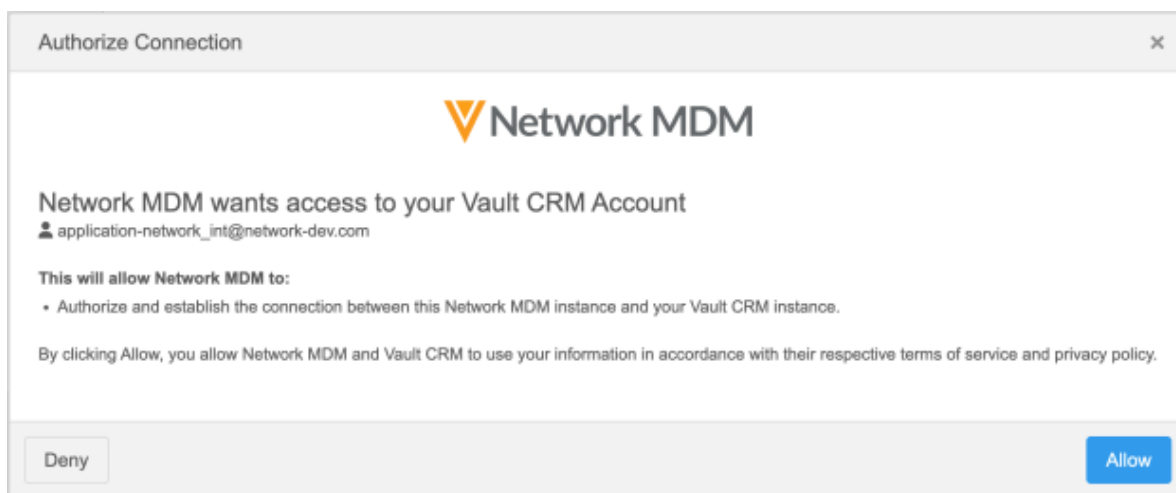
5. Click **Authorize Connection**.

Network MDM validates that the Vault CRM instance is configured to point to this Network MDM instance.

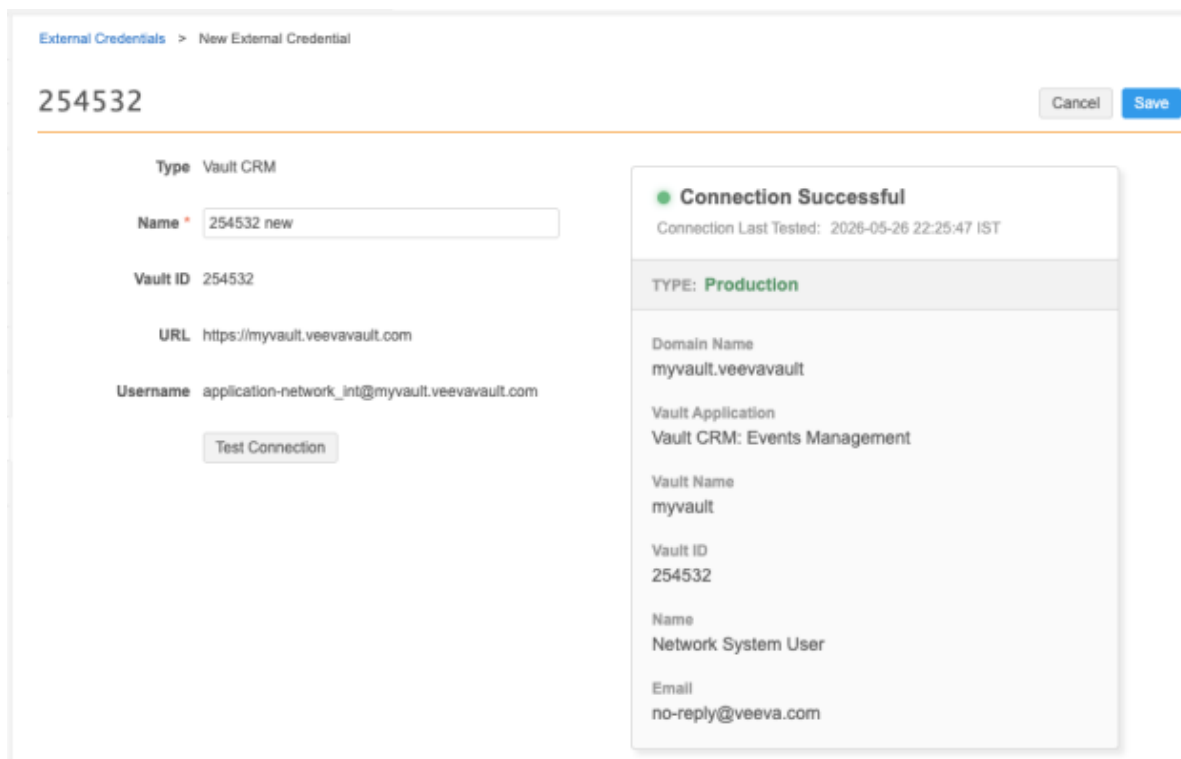


6. If the validation is successful, the **Authorize Connection** dialog displays.

Click **Allow** to confirm that you want to connect your Network MDM instance to the Network System User in Vault CRM.



7. The **Test Connection** action is automatically triggered. If the connection is made to Vault CRM, a success message displays.



8. **Save** your changes.



Update the Vault CRM Bridge

Change the credential used for the bridge so your bridge jobs continue to connect to Vault CRM.

- In a bridge configuration, expand the **External Credential** list and choose the credential under the **Vault CRM** heading.

My_Vault_CRM_Bridge Details [Start] [Cancel] [Save]

▼ Details

Name: My_Vault_CRM_Bridge

Type: Vault CRM Data Subscription

Status: ☒ Enabled ☐ Disabled

► Countries

► Network Data

▼ Connection Settings

The external credentials for the Vault CRM Integration User will be used to run the Network Bridge jobs.
If you have not created any credentials for your Vault CRM Integration User, [Click here](#)

❗ For integration with Vault CRM, it is recommended to select a Vault CRM external credential.

External Credential: 254532

▼ Advanced Settings

Revision Data Value (Optional):

Search [Q]

Vault CRM

164258

187431

254532

Vault

dcr-0130

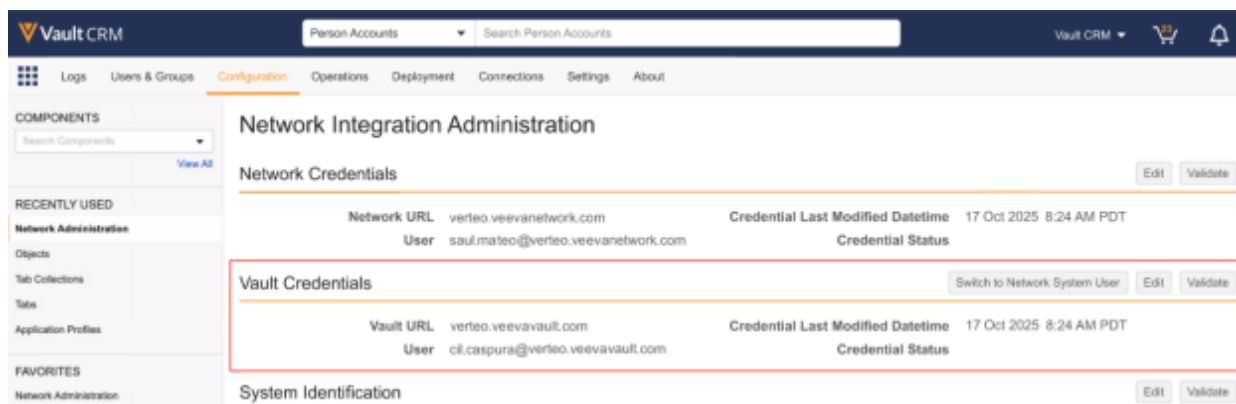
The bridge will now use the Vault CRM credential to connect to Vault CRM.



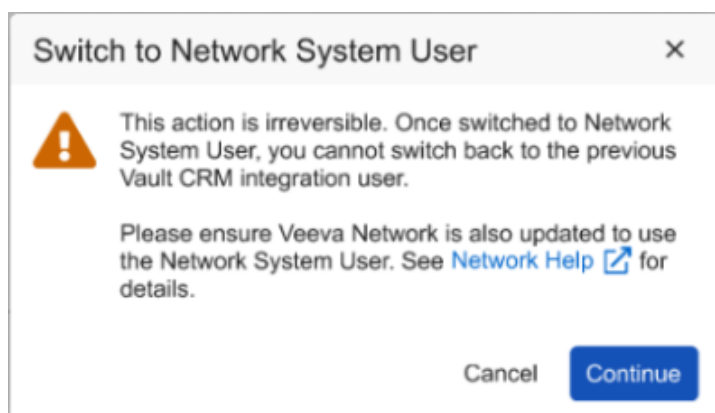
Switch to the Network System User

To start using the Network System User:

1. In Vault CRM, open the Network Integration Administration page (**Configuration**).



2. In the **Vault Credentials** section, click **Switch to Network System User**.
3. An alert displays to ensure that you understand that the change is not reversible. Click **Continue**.



The **Vault Credential** section updates to change the existing Vault Integration user credentials to the Network System User credentials.

Note: There is no **Edit** button for the **Vault Credentials** section. The Network System User cannot be changed.



Security

DYNAMIC USER PROVISIONING FOR SINGLE SIGN-ON (SSO)

26R2

Administrators have more flexibility for defining new users that are created using SSO. You can now use your SSO provider groups and countries to map to Network MDM settings and automatically set up new users with the correct access the first time they log in. This eliminates manual profile updates and ensures global users instantly receive the correct access and permissions.

Single Sign-On Settings [Edit](#)

▼ Auto-Creation of User Accounts

☒ Enable Auto-Creation of User Accounts

[▶ Test User Settings](#)

SAML MAPPINGS

VEEVA ATTRIBUTE	SAML ATTRIBUTE
Country	c
Email	mail
Federated Id	uid
First Name	fname
Last Name	sname
Group	group

MAPPINGS

☐ Use Country and DVP mappings

☒ Use a mapping file (Groups/Country support)

Upload a file to map your SSO Groups/Countries to Network MDM configuration settings.

User creation rules:

- **Data Visibility Profiles (DVPs):** Combine all unique DVPs from both Country and SSO mappings (duplicates removed).
- **User Groups:** Assign all user groups from both Country and SSO mappings.
- **Language, Locale, and Timezone:** User Country mappings first, then SSO mappings if needed.
- **User Type:** Grant highest available privilege (for example, Data Steward overrides Standard User).

PAST SSO MAPPINGS [past_mappings.zip](#)

CURRENT SSO MAPPINGS [sso_mappings.csv](#)
FILE UPLOADED

5 SSO GROUPS MAPPED

5 DATA VISIBILITY PROFILES MAPPED

3 NETWORK USER GROUPS MAPPED

1 USER TYPES: Standard User

This enhancement is enabled by default.

Important: This feature will be fully supported starting with the 26R2.0.1 Production release (August 21, 2026). User authentication is not supported when SSO is configured with groups for the Sandbox release.



Highlights

- **User group management** - Administrators can now map their existing identity provider groups (like Okta® or Microsoft® Azure AD) directly within the Network SSO configuration. This eliminates the need to manually add users to Network MDM groups after they are auto-created.
- **User type provisioning** - New users can now be automatically created as a Portal User, Standard User, or Data Steward. Previously, all new users defaulted to Standard Users and required manual updates.
- **Data access** - Users are automatically assigned to specific Data Visibility Profiles (DVPs), Network Portal applications, and permission sets based on their SSO groups.
- **Localization settings** - Key user preferences—including time zone, locale, and language settings—are now defined automatically using group rules, ensuring global users can work immediately without manual setup.

Updates for SAML mappings

A **Group** field is added to the SAML mappings so you can automatically assign a user to all of the groups that you have defined for that user in your SSO provider. This is an optional field.

SAML MAPPINGS	
VEEVA ATTRIBUTE	SAML ATTRIBUTE
Country *	c
Email	mail
Federated Id *	uid
First Name *	fname
Last Name *	sname
Group	group



Example for Microsoft Azure AD (Entra ID)

A user is assigned to the following groups.

The screenshot shows the 'Groups' page in the Microsoft Azure AD portal. A user is selected, and a list of groups they are assigned to is displayed. The groups are:

Name	Object Id	Group Type	Membership Type
albany office	91b46b3e-0513-4a2c-9a1a-12bd892e2c1e	Security	Assigned
data science	77386619-231a-452f-85a8-bffa5dcaf5c	Security	Assigned
Developers	2ecf3f27-d323-4078-a78c-dd83f89f8c43	Security	Assigned
KAMS	91568a03-7e6b-4354-bd27-3930e7462fef	Security	Assigned
Marketing	04929562-ac22-452e-a822-71790759ca1b	Security	Assigned

In your Azure AD SSO settings, copy the **group** property value, for example `group`.

The screenshot shows the 'SAML-based Sign-on' configuration page in the Microsoft Azure AD portal. The page is titled 'Set up Single Sign-On with SAML'. It includes a sidebar with navigation options like Overview, Deployment Plan, and Manage. The main content area shows the configuration details for the application.

Basic SAML Configuration

- Identifier (Entity ID): [Redacted]
- Reply URL (Assertion Consumer Service URL): 2333-1500-482f-9ab7-cac96c44b8a8
- Sign on URL: Optional
- Relay State (Optional): Optional
- Logout URL (Optional): Optional

Attributes & Claims

Attribute	Value
name	user.userprincipalname
sname	user.surname
fname	user.givenname
uid	user.userprincipalname
mail	user.mail
group	user.groups
c	"US"
Unique User Identifier	user.userprincipalname



Okta example

In your Okta SSO settings, copy the attribute name for your SSO groups. In this example, the name is "group".

Attribute statements

Learn more about configuring [attribute statements](#)

Add expression

Name	Expression	Actions
c	user.profile.countryCode	
fname	user.profile.firstName	
group	user.getGroups({'group.profile.name': {'Everyone', 'kams', 'CRM'}, 'operator': 'STARTS_WITH'}).! [profile.name]	
mail	user.profile.email	
sname	user.profile.lastName	
uid	user.profile.email	

Show legacy configuration

In the Network MDM **SAML Mappings**, add the SSO group attribute value to the **Group** field.

This will provide all your SSO group data to Network MDM. When users are created in Network MDM using SSO, the groups will be assigned to them.



Upload a file of your group mappings

There are now two options for defining the mappings between countries and data visibility profiles (DVPs) for automatically created users.

Mapping Option	Method	Details
Use Country and DVP mappings	Define the mappings between countries and DVPs. This is the default option that has not changed.	Recommended for use: Limited number of users in just one or a few regions. Supported user types: Standard Users only Maintenance: Administrators might need to manually update user permissions and modify user types.
Use a mapping file	Use the provided templates to upload a .csv file to map your SSO groups and countries to Network MDM settings.	Recommended for use: Many users that are located in global regions. Supported user types: Standard Users, Portal Users, and Data Stewards. Maintenance: User creation rules will automatically configure the country, DVP, and user types as defined in the uploaded file.

Define group mappings

To use the new option to upload a file of mappings, complete the following steps.

1. On the Single Sign-On page, click **Edit**.
2. In the **Mappings** section, select **Use a mapping file** (Groups/Country Support).
3. Click **Upload Group Mappings**.
4. In the dialog, click **Download Template**.

Upload Group Mappings

Step 1: Download Group Mappings template.

Download Template

Step 2: Update the group_mapping.csv file to map your SSO groups to Network configuration settings.

Step 3: Upload the edited group_mapping.csv file.

Drag edited file here (.csv)

or

Upload File



A compressed file called `SSO Mapping Template.zip` is downloaded to your local computer.

It contains three files:

File Name	Description
Group Mapping Instructions.txt	A plain text document that provides the instructions for defining your mappings.
network_configurations.xlsx	An inventory of the available configurations in your Network MDM instance (DVPs, User Groups, User Types, Timezones, Locales, and Languages). Use these values to populate the <code>sso_mapping.csv</code> file. Click the links to navigate directly to the configuration in Network MDM.
sso_mapping.csv	An empty file containing the column headers for the mappings. Define the mappings in this file and then upload to Network MDM.

- Open the `sso_mappings.csv` to define the mappings that Network MDM will use to automatically create users.

Add values for the following columns.

Column	Value	Details	Example
SSO_GROUP	Group name from your SSO provider.	Required if SSO_COUNTRY is empty.	91568a03-7e6b-4354-bd27-3930e7462fef
SSO_COUNTRY	Country (ISO 2-digit code) from your SSO provider.	Required if SSO_GROUP is empty. The value must match a country value in Network MDM.	FR



Column	Value	Details	Example
NETWORK_USER_TYPE	User type that will be set for these users. Available options: DS (Data Steward), SU (Standard User), PU (Portal User)	Optional Use the UserTypeID column from the network_configurations.xlsx file.	PU
NETWORK_DVPS	Data Visibility Profile (DVP) that users will be mapped to.	Required Use the DVPID column from the network_configurations.xlsx file. It includes all DVPs defined in your Network MDM instance. Multiple values are supported. Use double semi-colons (;;) to separate each value.	canada_data__c
NETWORK_USER_GROUPS	Custom Network MDM user groups to assign to users.	Optional Use the UserGroupID column from the network_configurations.xlsx file. It includes all custom groups that have been created in your instance. Multiple values are supported. Use double semi-colons (;;) to separate each value.	Marketing_Users__c;; KAM_Group__c
NETWORK_LOCALE	Network MDM locale to assign to users.	Optional Use the LocaleID column from the network_configurations.xlsx file. It includes all locales available in Network MDM.	en_CA
NETWORK_TIMEZONE	Timezone to assign to users.	Optional Use the TimeZoneID column from the network_configurations.xlsx file. It includes all timezones available in Network MDM.	America/Toronto
NETWORK_LANGUAGE	Language to assign to users.	Required Use the LanguageID column from the network_configurations.xlsx file. It includes all languages available in Network MDM.	en



Column	Value	Details	Example
APPLY_TO_EXISTING_USERS	Indicate the configurations to apply to existing SSO users when they log into Network MDM.	Applies only to NETWORK_DVPS and NETWORK_USER_GROUPS. Use double semi-colons (;;) to separate each value.	NETWORK_USER_GROUPS;;NETWORK_DVPS

Example sso_mapping.csv file

SSO_GROUP	Group Info	SSO_COUNTRY	NETWORK_USER_TYPE	NETWORK_DVPS	NETWORK_USER_GROUPS	NETWORK_LOCALE	NETWORK_TIMEZONE	NETWORK_LANGUAGE
91566a03-7e9b-4354-b127-3800x7462f4f	KAMs		PU	us_data__c		en_US	America/Toronto	en
77386619-231a-452f-85a9-b1ff55cafa5c	data science		PU	turkey__c;russia__c;usnodownload__c	Marketing_Users__c	en_CA	America/Sao_Paulo	en
77386619-231a-452f-85a9-b1ff55cafa5c	Developers		DS	us_data__c	Marketing_Users__c;KAM_Group__c	en_US	America/Toronto	en
91b46b3e-0513-4a2c-8a1a-12bd880e2c1e	allany_office			jersey__c				
04829592-ac22-452e-a822-71760799ca1b	Marketing			ru__r_data__c				

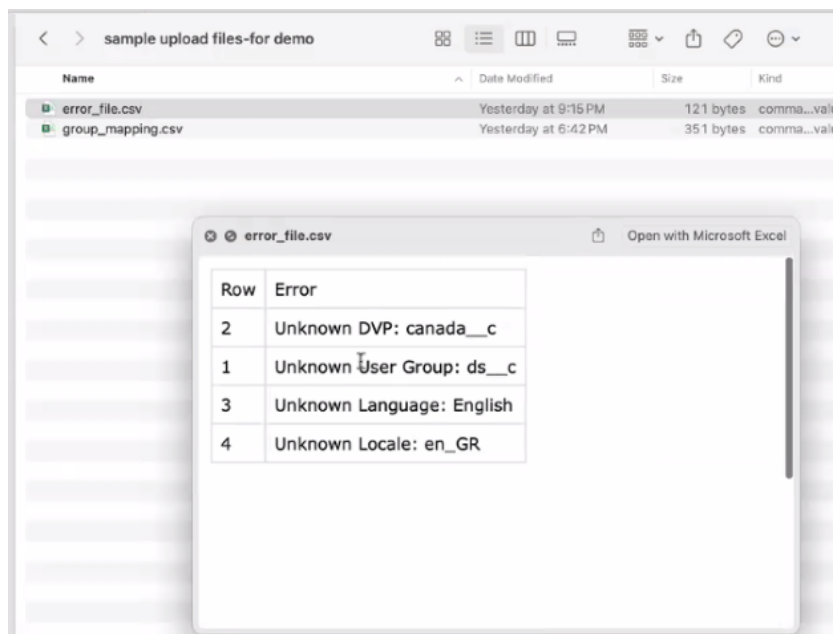
Tip: Additional columns can be included in the file. In this example the **Group_info** column is added to help describe the SSO group.

- When the mapping is complete, click **Upload File** to add the mappings in the .csv file to your SSO configuration.

The file is validated to ensure it contains the required information and it is in the expected format.

- File format** - .csv
- Required columns** - SSO_GROUP or SSO_COUNTRY, NETWORK_DVPS, and NETWORK_LANGUAGE.
- Values** - Values in the SSO_COUNTRY and NETWORK_ columns must match to the values defined in Network MDM. Use the *network_configurations.xlsx* file for all accepted values.

If you see validation errors, click **Download Error File** to view the issues. Make the changes and upload the updated file.





- When the file is uploaded successfully, the mapping results display a count of each mapped setting: SSO Groups, DVPs, User Groups, and User Types.

MAPPINGS

☐ Use Country and DVP mappings

☒ Use a mapping file (Groups/Country support)

Upload a file to map your SSO Groups/Countries to Network MDM configuration settings.

User creation rules:

- **Data Visibility Profiles (DVPs):** Combine all unique DVPs from both Country and SSO mappings (duplicates removed).
- **User Groups:** Assign all user groups from both Country and SSO mappings.
- **Language, Locale, and Timezone:** User Country mappings first, then SSO mappings if needed.
- **User Type:** Grant highest available privilege (for example, Data Steward overrides Standard User).

CURRENT SSO MAPPINGS [sso_mappings.csv](#) FILE UPLOADED [Re-Upload SSO Mappings](#)

5 SSO GROUPS MAPPED

5 DATA VISIBILITY PROFILES MAPPED

3 NETWORK USER GROUPS MAPPED

2 USER TYPES: Portal User, Standard User

The mapping file that you uploaded displays in the **Current SSO Mappings** section. The file can be downloaded any time by clicking the `sso_mappings.csv` file name.

- Save** your changes. The uploaded file will not be applied until the SSO configuration is saved.

Mapping rules

If the file includes **Country** and **Group** mappings, there are rules to understand which configuration will be applied when users are automatically created.

- **DVPs** - A combination of all unique DVPs from the **SSO_Country** and **SSO_Group** mapping columns are applied.
- **User Groups** - All user groups are applied.
- **Language, Locale, and Timezone** - Apply the first matching settings found in the mappings. If none are defined, apply the default settings in the SSO configuration.
- **User Type** - The user type with the highest privilege wins (for example, Data Steward overrides Standard User, Standard User overrides Portal User). If no user type is defined, the user will be created as a Standard User.

Additional rules

- If a row contains **SSO_Group** and **SSO_Country** values, the settings will apply only to users that have both. to both.
- If a row contains **SSO_Group** only, its settings will apply to any user matching that group, regardless of the country.
- If a row contains **SSO_Country** only, its settings will apply to any user matching that country regardless of their SSO group.



Updating the mappings

The mapping file can be updated at any time.

1. Click **Re-Upload SSO Mappings**.
2. In the dialog, choose to download the template or to download and edit your existing mapping file.

The dialog box titled "Re-Upload SSO Mappings" contains three steps:

- Step 1:** Download SSO Mappings template (empty) or your current SSO Mappings file. Below this are two buttons: "Download Template" and "Download Current SSO Mappings".
- Step 2:** Update the sso_mappings.csv file to map your SSO groups to Network configuration settings.
- Step 3:** Upload the edited sso_mappings.csv file.

Below the steps is a large dashed box containing a cloud upload icon and the text "Drag edited file here (.csv) or" followed by a blue "Upload File" button.

3. Upload the new or updated mapping file.
4. When the validated file is successfully uploaded, the displayed mappings reflect the new mappings.
5. Your previous mapping file can be downloaded in the **Past SSO Mappings** section.
6. **Save** your changes.

The dashboard shows the status of SSO mappings:

- PAST SSO Mappings:** A button to download "past_mappings.zip".
- CURRENT SSO Mappings:** Shows "sso_mappings.csv" as "FILE UPLOADED" and a "Re-Upload SSO Mappings" button.
- Summary Cards:**
 - 7 SSO GROUPS MAPPED
 - 8 DATA VISIBILITY PROFILES MAPPED
 - 4 NETWORK USER GROUPS MAPPED
 - 3 USER TYPES: Portal User, Data Steward, Standard User



Test the SSO configuration

After you have uploaded the mappings, you can test the SSO configuration to understand the Network MDM settings that will be applied to a user.

1. When the Single Sign-On Settings page is in read-only mode, click **Test User Settings**.
2. In the dialog, add the SAML attribute mappings. For the **group** field, add a group from your uploaded mappings file.

Click **Add Attribute** to include multiple groups.

Test User Settings

Enter sample SAML attribute values to see the settings and configurations the user will be created with.

SAML ATTRIBUTE	VALUE	
c	US	×
mail	sara.woods@verteo.com	×
uid	sara.woods@verteo.com	×
fname	sara	×
sname	woods	×
group	77386619-231a-452f-85a8-bffa5dcaf5c	×

[+ Add Attribute](#)

Evaluate

▼ Applied Configurations

CONFIGURATION	VALUE
Data Visibility Profile	Russia, Turkey, US
Language	English
Locale	Mexico
Timezone	(GMT+00:00) Greenwich Mean Time (GMT)
User Groups	Marketing Users
User Type	Standard User



3. Click **Evaluate**.
4. The **Applied Configurations** section displays the settings that will be applied to the user:
 - Data Visibility Profile
 - Language
 - Locale
 - Timezone
 - User Groups
 - User Type

Logs

Administrators can track the SSO mapping changes in the System Audit Log.

SSL CERTIFICATE UPDATE

26R2

The current SSL certificate for veevanetwork.com expires on September 13, 2026.

The following certificates must be updated before that date.

- **veevanetwork.com** - Covers all Sandbox and Production Network MDM instances and login.veevanetwork.com.
- **Intermediate CA certificate cert** - Ensures that the SSL certificate is fully trusted by the supported browsers and client computers.

Note: The certificates are not yet available. They will be added here when they are available in August.

Only customers who explicitly download and install certificates on any site caches or proxy servers must update their certificates.



API

VERSION UPDATE FOR 26R2.0

26R2

The Network API is updated to v40.0.

The Network API version is updated for every major release. Any additional changes are documented in this section of the Release Notes.

As with all version updates, Integration Users should continue to use v39.0 until there is a change for v40.0 that they want to apply.

For more information about the Network API, see the *Veeva Network API Reference* at <http://developer.veevanetwork.com>.

VERSION UPDATE FOR 26R1.1

26R1.1

The Network API is updated to v39.0.

The Network API version is updated in this release to support the [Master data disclaimer](#) feature.

As with all version updates, Integration Users should continue to use v38.0 until there is a change for v39.0 that they want to apply.

RESTRICT ACCESS TO AUTHORIZED SYSTEMS

26R1.1

The Change Request Search and Retrieve APIs now enforce the system access restrictions in your user profile, automatically limiting results to DCRs from your authorized systems. Previously, the Change Request API returned all DCRs.

Users » john.smith@verteo.veevanetwork.com

john.smith@verteo.veevanetwork.com

Cancel Reset Password Save

▼ Additional Permissions

API Access Selected Systems Only

Select the systems this user will have API access to

IQVIA OneKey X SAP X

Compliance Data Hide Preview box on profile

Data Lineage Display Preview box on profile

This enhancement is enabled by default in your Network MDM instance.



Access to systems

Administrators can define the systems that users have API access to in each user profile.

1. In the **Additional Permissions** section, choose **Selected Systems Only** for the **API Access** setting.
2. In the field, add the systems.

When an API request is made to search or retrieve third-party master DCRs, the DCRs will be filtered by the list of authorized systems in the user's profile. If the user's permission is set to **All Systems**, the API will continue to return all DCRs.