Veeva Network

Veeva Network 17R2.0.1 Release Notes

August 2017

Contents

About these Release Notes **8**

Browser requirements **8**

Release Note updates **8**

What's new **8**

Managing configurations 8

Data load 8

Data lineage 8

Data visibility profiles 9

Inbox 9

Suspect match 9

Match 9

Network explorer 9

Profile 9

General updates 9

API 9

Data Governance 9

Veeva OpenData subscriptions 10

Users 10

Network address inheritance 10

Network Explorer 10

Inbox 10

Data load 10

Match 10

Data maintenance 11

Data change requests 11
Home dashboard 11
General updates 11
Reports 11
Ad hoc match 11
Concur Connector 11
Logs 12
Introduction 13
Network Customer Master 13
Network configurations 14
Exporting configurations 14
Ad hoc download 15
Create a new package 16
Review packages 19
Downloading packages 19
Cloning packages 20
Importing configurations 20
Data load 24
Deduplicating child objects 24
Matching child objects 24
Child object deduplication examples 25
Deduplicate child objects 27
Job properties 27
Job settings summary 27
Match analysis logs 28

Example 30
Log file names 31
Advanced job property 31
Data provider confirmation 32
Audit 32
Data lineage 33
Filtering by source 33
Data visibility profiles 34
Filtering records 34
Filter options 35
Filter records using data visibility profiles 35
Inbox 36
Saving views 36
Enabling this feature 36
Creating inbox views 37
Select saved views 39
Update views 39
Reset views 39
Edit view names 40
Delete views 40
Auditing 41
Selecting and resetting columns 41
Task details 42
Network address inheritance 43
Refreshing child addresses 43

Scheduling updates to refresh addresses 43
Revision history 45
Suspect match 46
Selecting surviving fields 46
Usability enhancements 47
Selecting fields 48
Data lineage 49
Revision history 50
Match 51
Add request match rules 51
Defining match rules 52
Substring algorithm tooltip 53
Monge Elkan algorithm 53
Pinyin Jaro algorithm 54
Match configuration for China supported in Basic mode 54
Match on Parent HCO records 55
Selecting null fields in data groups 55
Data groups with null values 57
Home dashboard 57
Feature enabled 57
No widget data 57
No widgets found 57
Unavailable widgets 58
Data explorer updates 58
New widget 59

Refreshing the home dashboard 59
Refreshing individual widgets 60
Network Explorer 60
Wrap entity names 60
Profiles 61
Inactive objects 61
Users 61
Feature access settings 61
Search 63
Data maintenance 64
Child object inactivation 64
Data change requests 64
Alternate keys 64
Associated tasks 65
Resolution notes 65
General updates 66
POD information 66
POD details 67
Starred entities 67
Reports 67
Reports tab 67
Ad Hoc Match 67
Concur Connector 68
Field mappings 68
Mapping the State address field 68

Child objects in search results 68

Filter search results 70

Connection settings 70

Logs 71

Search audit history 71

API 71

Search API 71

Parameters 71

About these Release Notes

These Release Notes describe all features that are included in Veeva Network 17R2.0.1.

Browser requirements

The following are the minimum browser requirements:

- Internet Explorer 11+
- Google Chrome (most stable version at Network release)
- Safari 6+

Veeva Network is not supported on mobile devices.

Release Note updates

The following topics have been added to the Release Notes since the Early version was published:

- **POD information** - Administrators can now see the POD information for their Network instance in the General Settings.

All material in the Release Notes should be reviewed to ensure that updates to existing topics are noted.

What's new

The following key enhancements have been introduced in Veeva Network since 17R1.2.

MANAGING CONFIGURATIONS

- **Exporting** - Configuration packages can be created and sent to target environments.
- **Importing** - Exported configuration packages can be deployed on target environments.

DATA LOAD

- **Deduplicating child objects** - Administrators and data managers can deduplicate child objects from records on incoming source feeds.
- **Match analysis logs** - Match logs can now be created for child objects (addresses, licenses, and Parent HCOs).

DATA LINEAGE

- **View by source** - Users can now filter the view by source system or individual custom keys.

DATA VISIBILITY PROFILES

- **Filtering records** - Administrators now have more flexibility for filtering HCP and HCO records that users can access.

INBOX

- **Saving configurations** - Data stewards, data managers, and administrators can now save inbox views to easily manage inbox tasks.
- **Selecting and resetting columns** - The columns options are now easily accessible using a new button in the inbox.

SUSPECT MATCH

- **Pick surviving values** - Data stewards and data managers can override survivorship rules and select individual field values to retain on surviving records.

MATCH

- **Advanced button** - The button to access the XML for match features has been renamed.

NETWORK EXPLORER

- **Wrap entity names** - This setting is now enabled by default in all Network instances.

PROFILE

- **Inactive objects** - The font color for values is darker and more easy to read.

GENERAL UPDATES

- **PODs** - Administrators can now see the POD information for their Network instance in the General Settings.

API

- **Search API** - The Search API is updated to include three new parameters and enhancements to the Filters parameter.

DATA GOVERNANCE

Specific updates for fields and reference data are provided in the *Veeva Network Data Governance* release notes.

The following key enhancements were introduced in Veeva Network 17R1.1 and 17R1.2.

VEEVA OPENDATA SUBSCRIPTIONS

- **Filter records** - Administrators can now more easily use filters to exclude records based on specialty and HCO/HCP type.

USERS

- **Feature access settings** - Administrators can simplify the Network UI for users by disabling some features.
- **Search** - Administrators can now search the Users, Inbox Task Groups, and Data Visibility Profiles lists.

NETWORK ADDRESS INHERITANCE

- **Address refresh** - Administrators and data managers can run jobs to refresh child addresses that are out of sync with parent addresses.

NETWORK EXPLORER

- **Wrap entity name setting** - Users can enable this setting so that nodes display the entire entity name.

INBOX

- **Suspect match** - The Task Details section now provides information about how the task was created.

DATA LOAD

- **Subscription questions** - When subscriptions are created, users must answer questions about the origin of the data.

MATCH

- **Add Request Match Configuration** - Administrators can now customize the match configuration for add requests for their Network instance.
- **Substring algorithm** - A tooltip has been added to help users define negative substrings algorithms in their match configuration.
- **Monge Elkan algorithm** - Sub algorithms can now be embedded into the Monge Elkan algorithm.
- **Pinyin Jaro algorithm** - This algorithm can now be configured in Basic mode.
- **Match rules for China** - The default match rules can now be viewed and managed in Basic mode.
- **Match on Parent HCO** - Match rules can now be configured to match on parent HCO records.
- **Null fields in data groups** - Null field values are now grouped by entity and child object so that data groups can be processed more efficiently.

- **Data Groups with null values** - Incorrect behavior with data groups being created with null values when the option is false is corrected.

DATA MAINTENANCE

- **Child inactivation** - Some of the sections on the Job Details page are renamed to clarify their purpose.

DATA CHANGE REQUESTS

- **Alternate keys** - Users can no longer submit alternate keys in an add request.
- **Associated tasks** - The Job ID now displays so data stewards can click it to open the DCR from the profile page.
- **Resolution notes** - Notes can now contain line breaks so that comments are more readable.

HOME DASHBOARD

- **No widget data** - Widgets that do not contain data now provide tips on data availability.
- **No widgets found** - If all widgets are removed, a message displays with tips for adding widgets.
- **Unavailable widgets** - If a widget is unavailable, a message displays to explain that it is temporarily unavailable.
- **Data explorer updates** - Usability enhancements have been added for this widget.
- **Dashboard cache** - By default, the dashboard is cached for 60 minutes.
- **Refreshing widgets** - Users can refresh individual widgets.

GENERAL UPDATES

- **Starred entities** - Users can now access their starred entities from the Network navigation bar.

REPORTS

- **Reports tab** - If the Reporting feature is not enabled in your instance, the tab does not display in the Network menu bar.

AD HOC MATCH

- **Ad Hoc Match tab** - If users do not have access to this feature through their data visibility profile, the tab does not display on the Network menu bar.

CONCUR CONNECTOR

- **Field mappings** - Mapping suggestions are no longer included in the field name; for example, Custom 14 (NPI Name).
- **Child objects in search results** - Network now returns the most relevant child objects based on the user's search criteria.

- **Filter search results** - The Concur Connector now includes a new section where users can filter their search results by country and record status.
- **Connection Settings** - The Concur Connector now includes the Concur URL which can be customized.

Logs

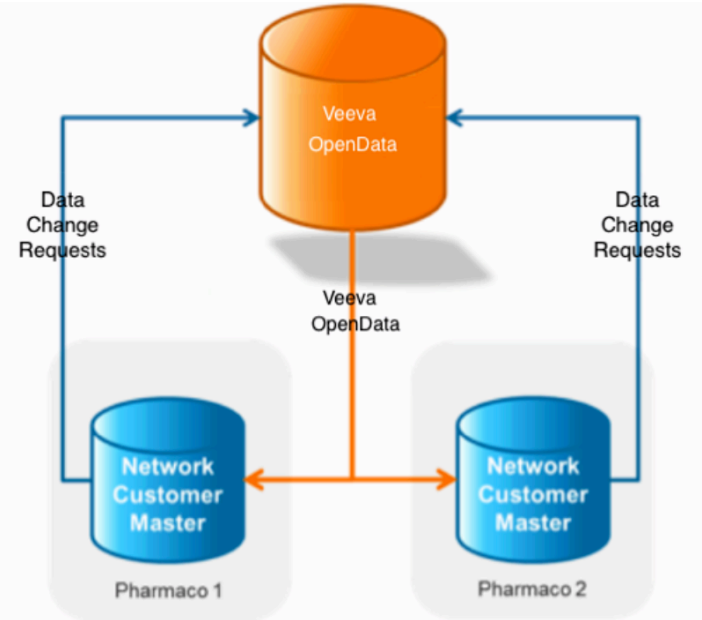
- **Search audit history** - The search log now contains filters and field queries.

Introduction

Veeva Network includes Network Customer Master, and for applicable countries, Veeva OpenData Customer Data.

Veeva OpenData provides identity, demographic, and licensure data about Healthcare Professionals and Healthcare Organizations.

Network Customer Master is a SaaS Master Data Management (MDM) application that is populated with a subset of the data from Veeva OpenData, according to each pharmaco's contract with Veeva.



Network Customer Master

Veeva Network Customer Master is a multi-tenant SaaS Master Data Management (MDM) application. Each pharmaco that subscribes to Veeva Network has its own Network Customer Master tenant (often referred to as a Network org similar in concept to a Veeva CRM or Salesforce.com org).

Where Veeva OpenData is enabled, each Network org comes pre-populated with data from the Veeva OpenData databases to which the pharmaco has subscribed. Veeva Network automatically keeps the data in each production Network org up-to-date and in sync with the data in Veeva OpenData.

Pharmacos can also load their own data into their Network org and match and merge it with the Veeva OpenData data. Veeva is responsible for stewarding the quality of the Veeva-provided data as well as any new records added in the Network org that can be shared with Veeva OpenData.

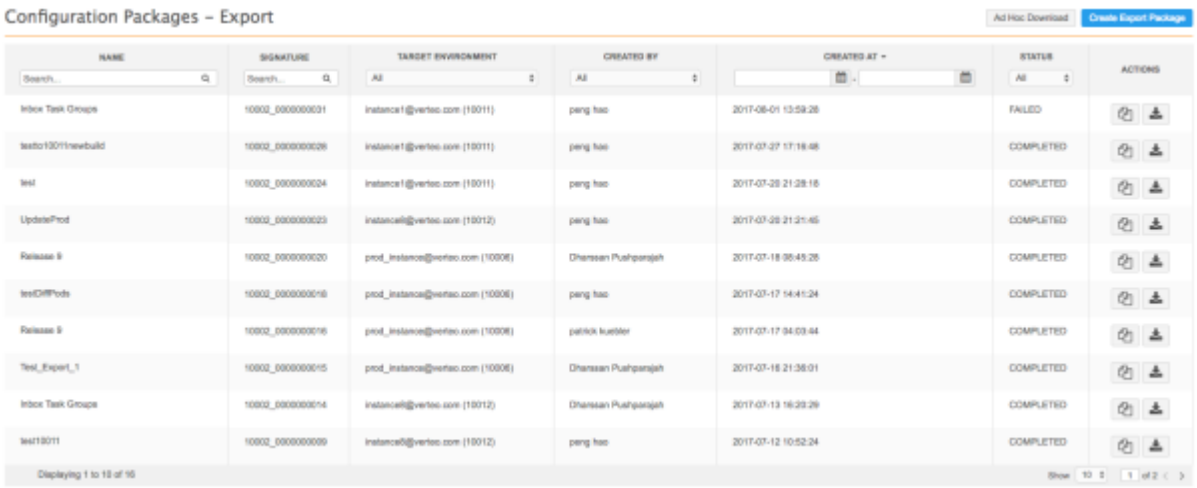
Records that do not match Veeva records will be loaded as customer-stewarded records and updates on those records will not be shared with Veeva OpenData.

Network configurations

In this release, administrators can now export Network configurations to target environments. Previously, administrators could download Network configurations as a file to their local computer and check for differences between environments. Now, exported packages can be created and exported to a Network target environment, eliminating the need to do configuration updates manually.

Importing configurations to a target environment has the following benefits:

- Ensures that the process is transparent, documented and auditable.
- Ensures that only authorized users can make deployments to target systems.
- Manages the complexity of dependent configuration objects.
- Ensures that deployments are non-disruptive to target system processes.



This feature is not enabled by default. To enable the feature for your Network instance, contact Veeva Support.

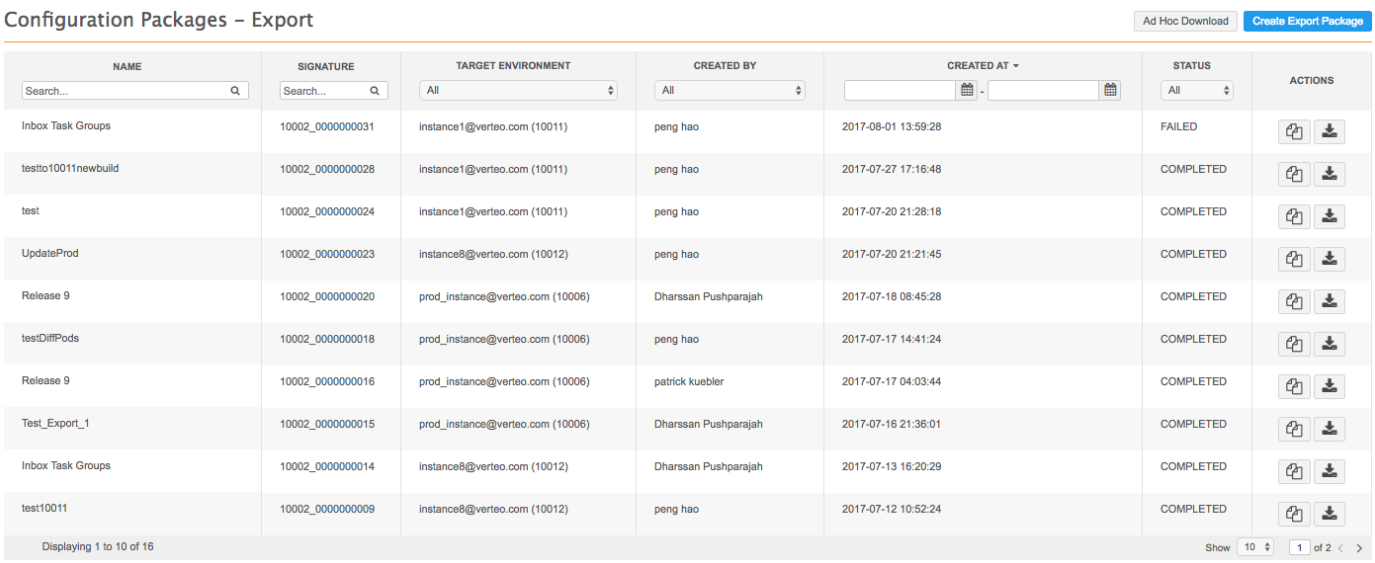
If the feature is not enabled, exporting configuration packages as an ad hoc download to your local server is still available, as usual.

EXPORTING CONFIGURATIONS

Administrators can create configuration packages to export to a target environment. The source and target environments must not be on the same Network release version.

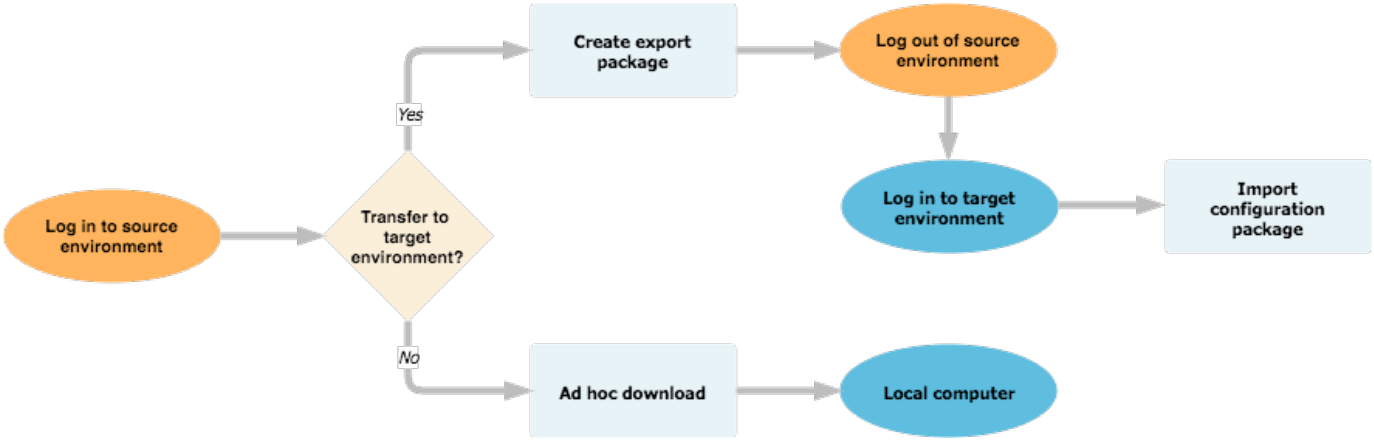
The Configuration Packages - Export page (**Settings > Export Configurations**) displays a list of all packages that were transferred from this Network instance to a target environment. The list is empty until you begin creating packages. In the **Status** column, you can see whether the package was successfully transferred (COMPLETED) or failed during the transfer (FAILED). Package deployments can fail if the target environment server was not available, or if the package could not be persisted in the target environment's database.

Packages that were downloaded as a .zip file but were not transferred to a target environment (using **Ad Hoc Download)** are not persisted and do not display in the list.



The following actions are available on the Configuration Packages - Export page:

- **Ad Hoc Download** - Create a .zip package to download locally.
- **Create Export Package** - Create a new package to export to a target environment.



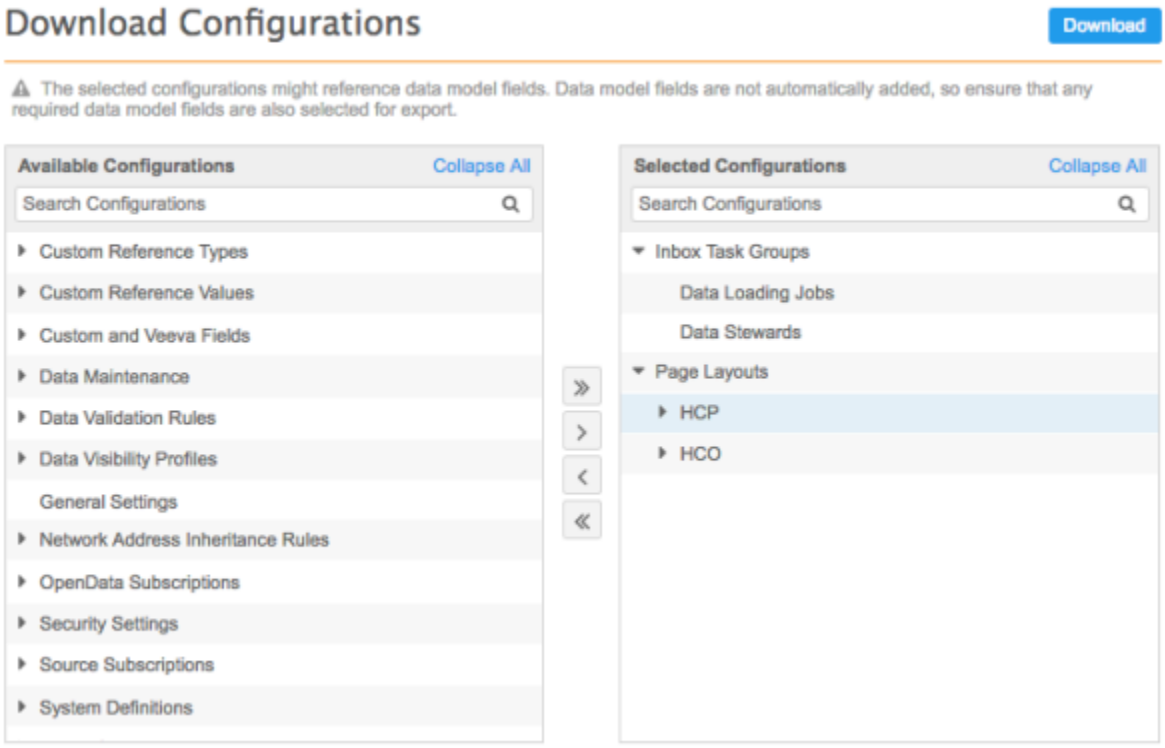
Ad hoc download

Downloading the configuration package as a .zip file is also useful for saving a snapshot of the current configuration. Imported configurations cannot be rolled-back after they are deployed on the target environment, so it's recommended to have this file saved for reference.

Ad hoc downloads cannot be imported to a target environment. They are intended only for doing line-by-line comparisons and for documentation purposes.

To download a package for comparing configurations between environments using a third party diff tool:

1. On the Configuration Packages - Export page, click **Ad Hoc Download**.



   The Download Configurations page opens so you can select the configurations that you want to include in the export file.

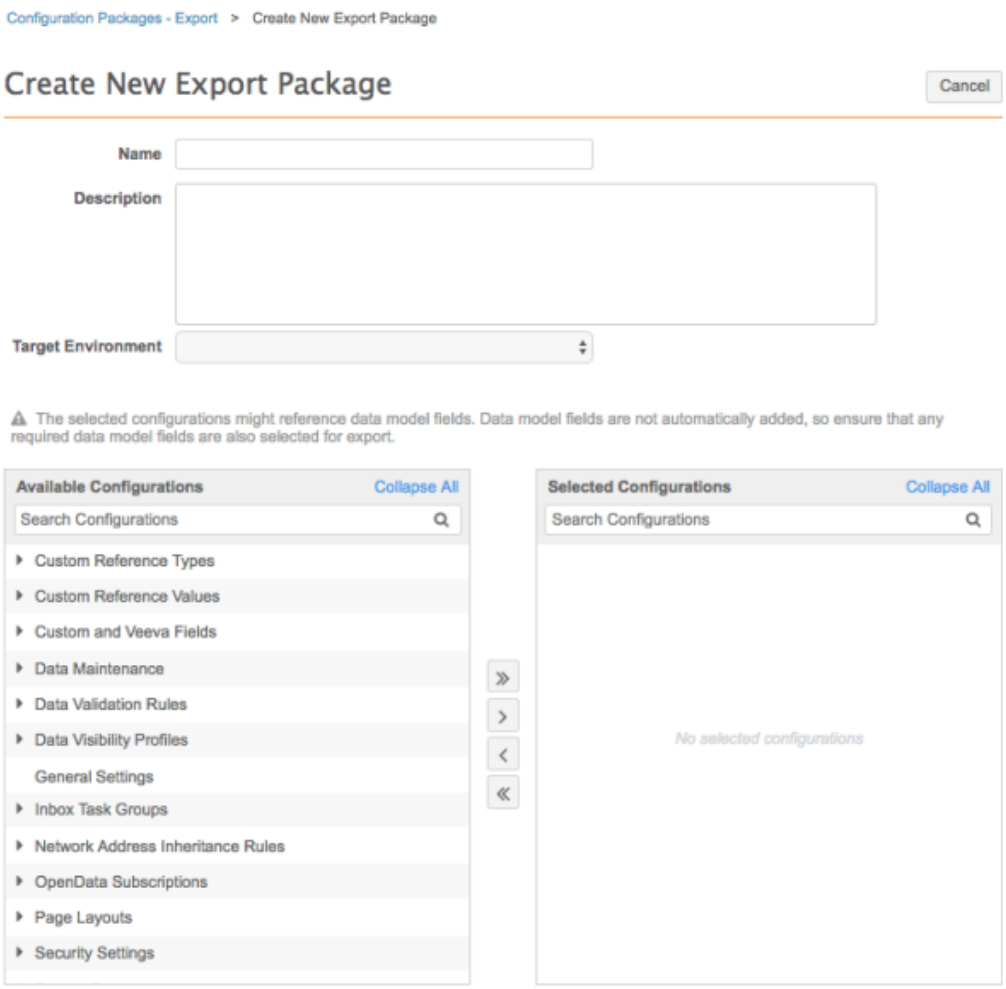
2. Move the configurations from the **Available Configurations** column to the **Selected Configurations** column. All dependencies for the selected configurations will be automatically added, except for dependencies for data model fields.
3. Click **Download** to export the .zip file to your computer. Now you can use a third party diff tool to do a line-by-line comparison with configurations downloaded from another environment.

Exports that are downloaded, and not deployed to a target environment, do not display in the list of packages on the Configuration Packages - Export page.

Create a new package

To deploy a set of configurations to a target environment, create an export package.

1. On the Configuration Packages - Export page, click **Create Export Package**.

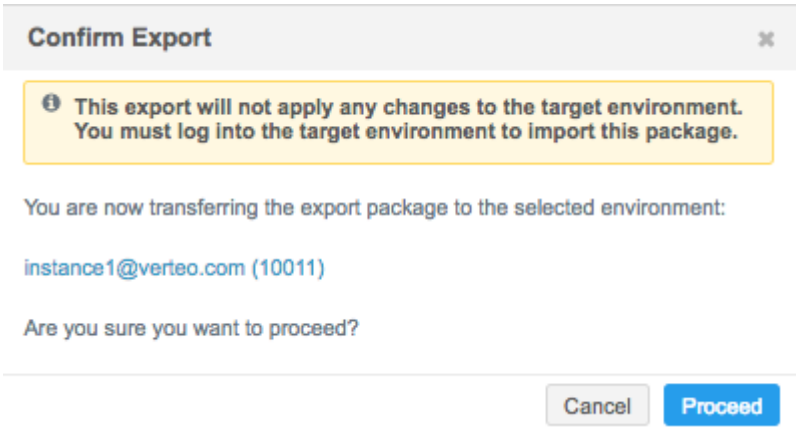


2. On the Create New Export Package page, define a name and a description for the package.
3. In the **Target Environment** list, select the server to export the package to.

   The list is pre-populated with a list of available environments. Each environment on the same domain can be a source or a target environment at the same time, enabling bi-directional deployment of configurations.

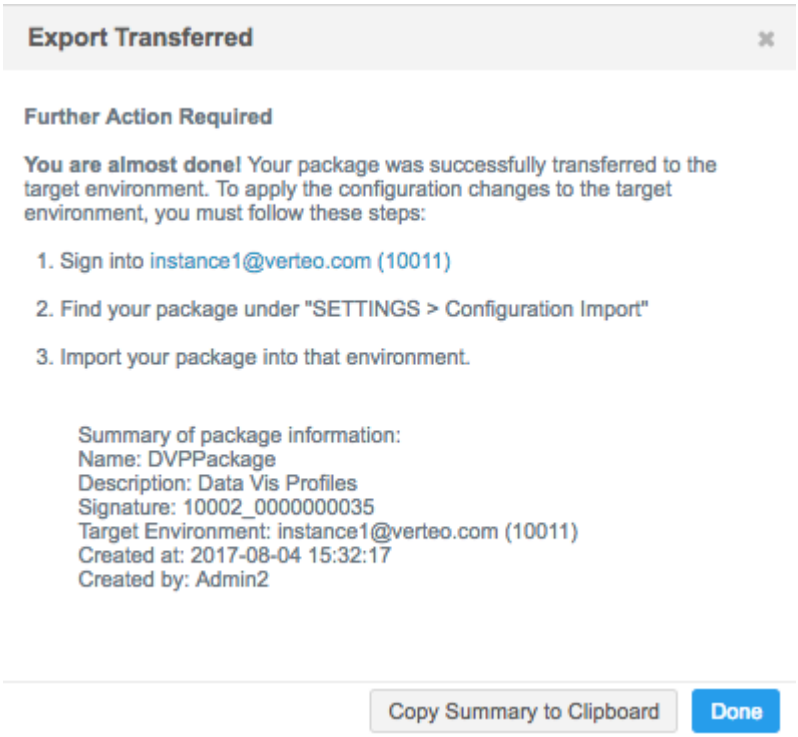
   If the list contains targets that should not be available for package deployment (for example, POC environments), contact Veeva Support to request that they be removed from the list. Veeva Support can also manually add any target environments that are missing from the list.

4. Select the configurations to export by expanding the categories in the **Available Configurations** pane and moving your selections to the **Selected Configurations** list. The selections are validated to check for dependencies. Dependencies, except dependencies for data model fields, are automatically added to your selections. If you remove configurations from the selection, the package must be validated again by clicking the **Validate** button.
5. Click **Export** to deploy the package to the target environment.
6. On the **Confirm Export** dialog, ensure that the target environment is correct. Click **Proceed**.



The configuration package is transferred to the target environment, but the configuration is not applied to the target. The changes are only applied when the package is imported on the target environment.

7. The **Export Transferred** dialog provides the status of the export, a summary of the package, and details for importing the package to the target environment. Click **Done**.



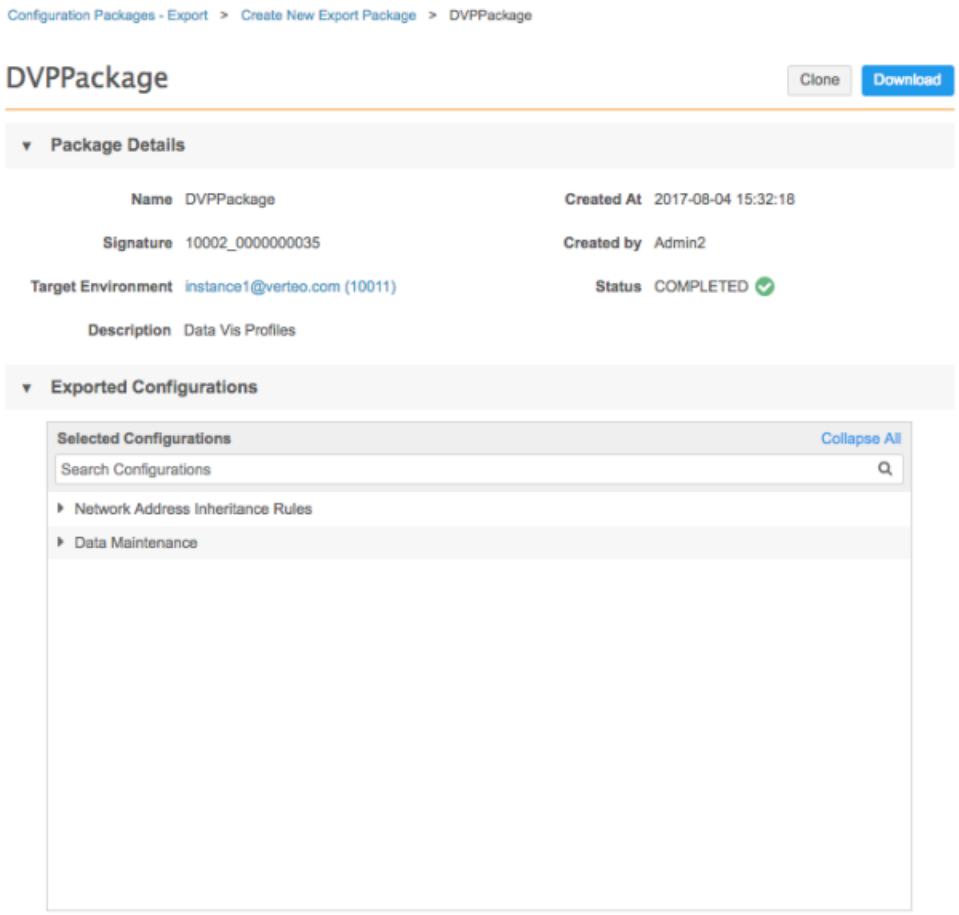
See *Importing configurations* to learn how to import the package to the target environment.

When the configuration package has been exported to the target environment, it displays in the list on the Configuration Packages - Export page. You can review, download, and clone exported packages that are listed on the page.

Review packages

Persisted packages can be opened so that you can review the package details. To open a package, click a package in the list.

All of the information on the details page is read-only. You can download the package using the **Download** button.



Downloading packages

Administrators can download .zip files of packages that have previously been transferred to a target environment. To download the package, click the **Download** icon .

Using a text editor to look at the JSON files, you can view the detailed configurations that the package contains. You can also compare the content of the package with the content of a second package, that was previously exported, by doing a line-by-line comparison in a third-party diff tool.

Cloning packages

If you want to use the same selection of configurations from a previous package and export it to the same or a different target environment, you can clone a package. Cloning is helpful for the following situations:

- Deploy a configuration to two separate test environments.
- Syncing the same target environment with updates in the current environment
- Redeploying a package that failed. Deployment can fail if the target server was unavailable.

To reuse a package:

1. In the package row, click the **Clone** icon .
2. On the Clone Package page, the name, description, target environment and selected configurations are pre-populated with the values of the cloned package. Change any of the existing values, if required.
3. Optional. Make any changes to the selected configurations.
4. Click **Export** to transfer the cloned package to the selected target environment.

IMPORTING CONFIGURATIONS

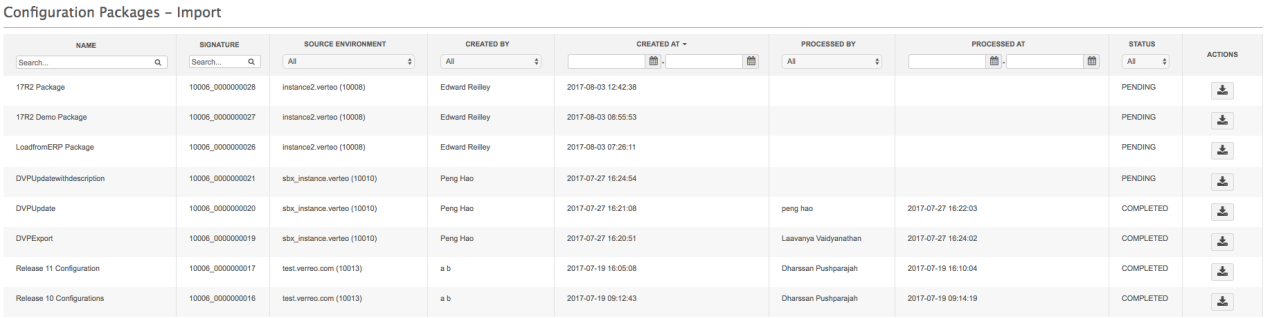
Administrators can import packages that have been deployed to their Network instance.

Note: Before applying the imported package to the target environment, use the **Ad Hoc Download** (**Configuration Packages - Export**) to take a snapshot of your current configuration so that you can refer back to it in case there are issues with the imported configuration. The snapshot can help you to troubleshoot any issues.

To import a configuration package:

1. In the Admin console, click **Settings > Import Configurations**.

   The Configuration Packages - Import page lists any packages that have been imported to your environment.



The table contains the following information:

Name - The package name.

Signature - The unique identifier of the package. This consists of the Network instance ID and an incremental package ID.

Source Environment - The instance where the configuration package was created.

Created By - The user who created the configuration package in the source environment. This user might not exist on the target environment.

Created At - The time that the package was created in the source environment.

Processed By - The user who imported the package.

Processed At - The time that the package was imported to the target environment.

Status - The configuration package status. The status can be one of the following:

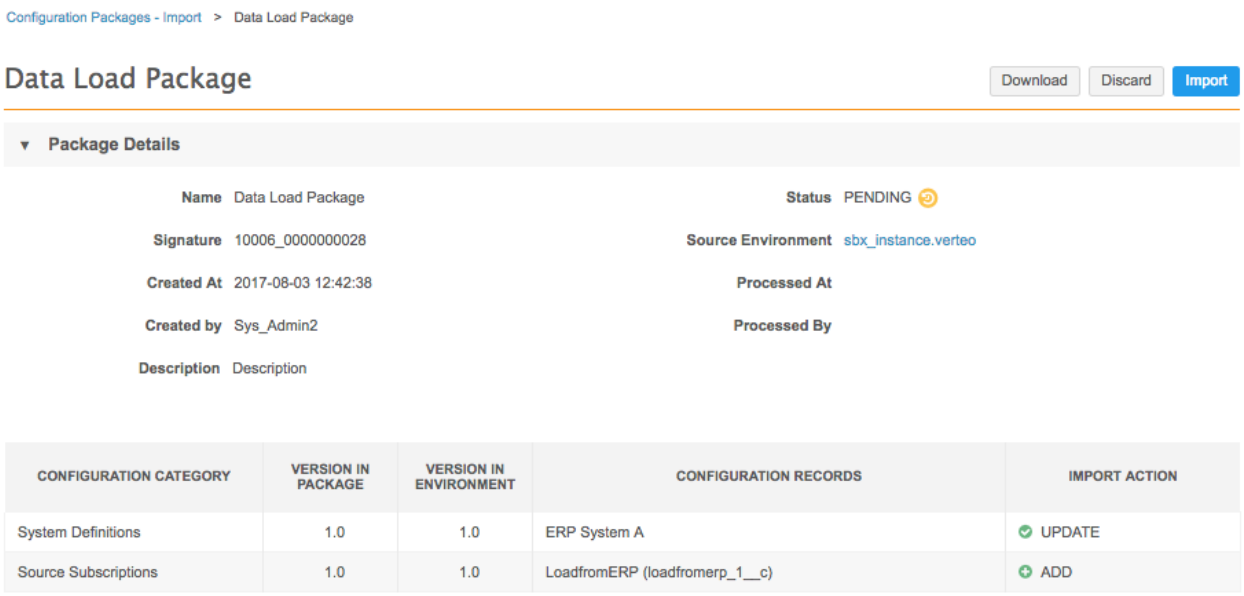
- **Pending** - The package has been transferred to the target but has not yet been imported.
- **Completed** - The package was imported.
- **Failed** - The package failed to be imported to the target.

Actions - The package can be downloaded.

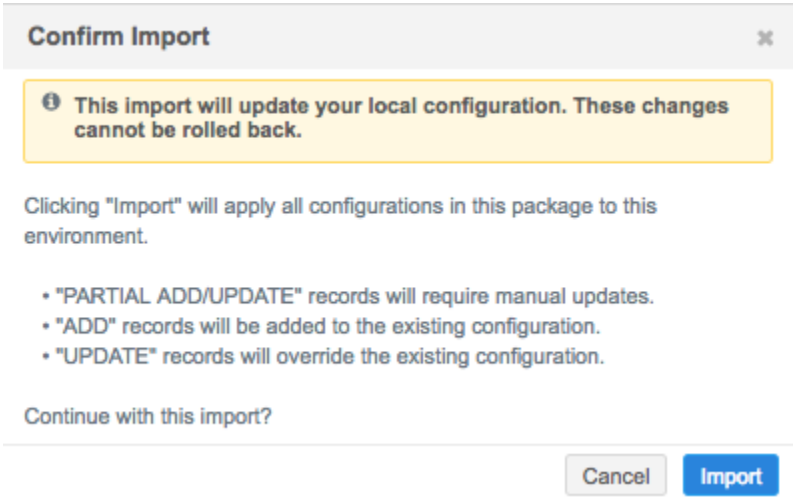
2. Click a package that is in **Pending** state.

   The package contains details about the configuration records that are included and what action will be taken during import. An **Import Action** can be one of the following:

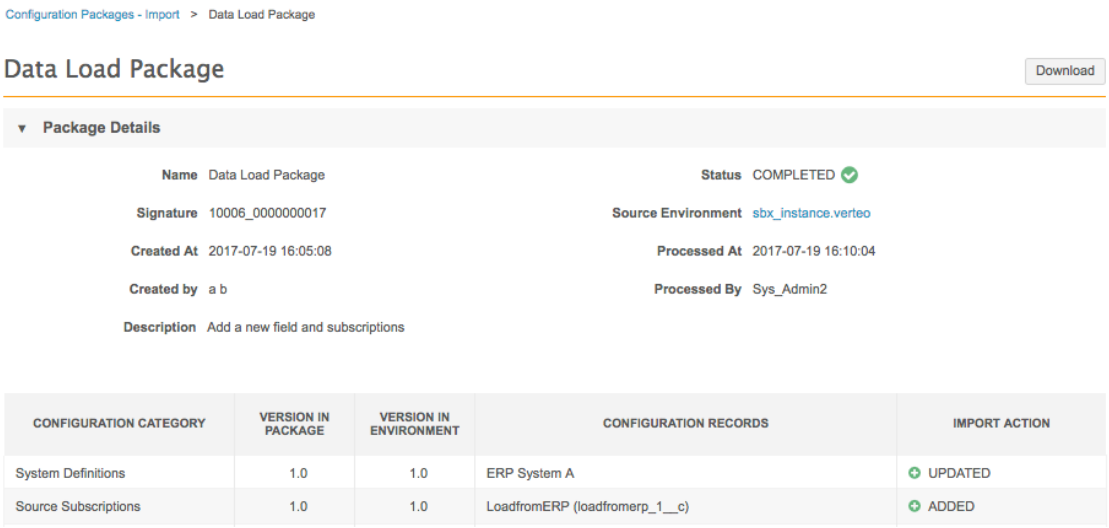
   - **Add** - Configuration records that do not exist in the target environment will be added.
   - **Update** - Configuration records that exist will be overridden.
   - **Partial update** - Some configuration records will be skipped or ignored, so they will have to be manually updated. For example, **General Settings** are typically partially updated because they contain feature flags that must be configured in the instance. When records are partially updated, you can see which records are skipped or ignored so that you can manually update them after the import.
   - **Partial add** – Some configuration properties are skipped during the add. For example, some single sign-on (SSO) settings are skipped.
   - **Skipped** - The complete configuration is skipped during the import. Configurations are skipped if the feature (for example, Concur) is enabled in the source environment but is not enabled in the target environment. The Concur settings will not be imported.



3. In the **Confirm Import** dialog, click **Proceed**.

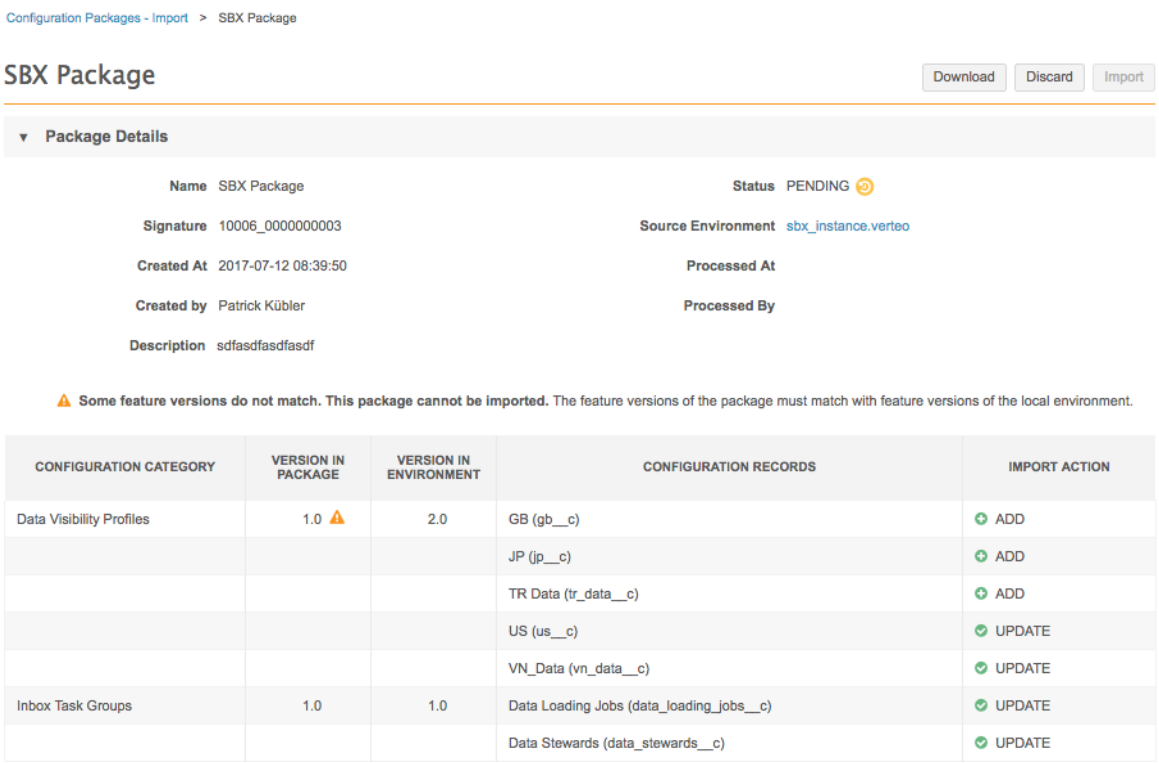


When the package is imported, the status updates to **Completed** and the **Processed At** and **Processed By** fields are populated.



Considerations during import

- If individual configuration records fail to be imported, the entire configuration package does not fail.
- If there is a mismatch between the version in the package and the environment, the **Import** button is dimmed and the package cannot be imported. Configurations must contain the same feature versions to be compatible. Versions change when there are significant enhancements to a feature.



Data load

The following topics describe enhancements to source subscriptions for this release.

DEDUPLICATING CHILD OBJECTS

Administrators and data managers can now choose to merge any duplicate child objects that are loaded during a source subscription job. Previously, HCP and HCO duplicates could be merged, but any child objects (addresses, licenses, Parent HCOs and custom keys) were retained on the winning record. Now, source subscriptions contain an option to merge duplicate child objects so that data quality is improved.

Child object deduplication is not enabled by default in new or existing source subscriptions. Administrators and data managers can select the option in the source subscription settings.

This feature does not deduplicate existing child objects in your Network instance. It applies only to data that is loaded through source subscriptions after the feature is enabled in each subscription. Child object duplicates cannot be matched and merged in Veeva OpenData or third party source subscriptions.

Matching child objects

Duplicate child objects are matched and merged using key matching (custom keys are the same) and field matching (using duplicate detection rules). Key matching is not available for Parent HCO child objects; they are matched using field matching or duplicate detection rules.

Duplicate detection rules

Network contains a set of default duplicate detection rules. Network uses the following fields for each child object to compare for duplicates. These rules are not visible in the Network UI.

Address	License	Parent HCO
If the address verification status is (V, A, P) • thoroughfare__v • premise_number__v • locality__v • country__v • postal_code_primary__v (except in China, use administrative_area__v instead) Any other verification status • address_line_1__v • locality__v • country__v • postal_code__v	license_number__v type_value__v license_degree__v	parent_hco_vid__v relationship_type__v hierarchy_type__v

For child object source deduplication, if duplicate child objects exist (there's more than one match) then Network breaks the tie by matching the objects to the best child object based on the following criteria:

- **Address**: status, `ordinal__v`, lowest Network Entity ID (VID)
- **License**: status, `best_state_license__v`, lowest VID
- **ParentHCO**: status, `is_primary_relationship__v`, lowest VID

Child object deduplication examples

Review the following examples to understand how Network deduplicates child objects.

Example 1 - Deduplicating entities and child objects using duplicate detection rules

In this example, multiple HCPs are loaded with the same address multiple times. The HCPs have already been determined to match and merge.

The custom key uses the following configuration:

- Source: SAP
- Item: ADDRESS
- Value: Network ID (VID)

HCP

VID	First Name	Last Name	NPI Number	Custom Key
59259	Bob	Smith	9925125	SAP:HCP:59259
7513B	Bob	Smith	9925125	SAP:HCP:7513B

Address

VID	Address_ID	Address Line 1	City	ZIP	Country	Custom Key
59259	4292151	123 Main Street	Salem	97310	United States	SAP:Address:4292151
59259	4292152	123 Main Street	Salem	97310	United States	SAP:Address:4292152
20012	4292153	123 Main Street	Salem	97310	United States	SAP:Address:4292153
20012	4292154	123 Main Street	Salem	97310	United States	SAP:Address:4292154

Result

When the data is loaded, Network first checks the custom keys for matches. In this example, the keys for the HCP and the Address do not match. Network uses the duplicate detection rules to determine if the objects are duplicates. The addresses are the same so one address is loaded. In this example, the address with VID 20012 wins because it was the last row to be added. All of the custom keys are added to the child object.

HCP

VID	First Name	Last Name	NPI Number	Custom Key
VID1	Bob	Smith	9925125	SAP:HCP:7513B SAP:HCP:59259

Address

VID	Entity_ID	Address_ID	Address Line 1	City	ZIP	Country	Custom Key
VID1A		4292154	123 Main Street	Salem	97310	United States	SAP:Address:4292154 SAP:Address:4292153 SAP:Address:4292152 SAP:Address:4292151

Example 2 - Duplicate detection rules

A record is loaded with duplicate addresses. There are no duplicate custom keys, so Network uses duplicate detection rules to deduplicate the child objects.

The custom key uses the following configuration:

- Source: SAP
- Item: ADDRESS
- Value: Network ID (VID)

VID	Address Line 1	City	ZIP	Country	Phone	Custom Key
2215A	123 Main Street	Salem	97310	United States	978-224-5000	SAP:Address:2215A
7513B	123 Main Street	Salem	97310	United States	351-555-0000	SAP:Address:7513B

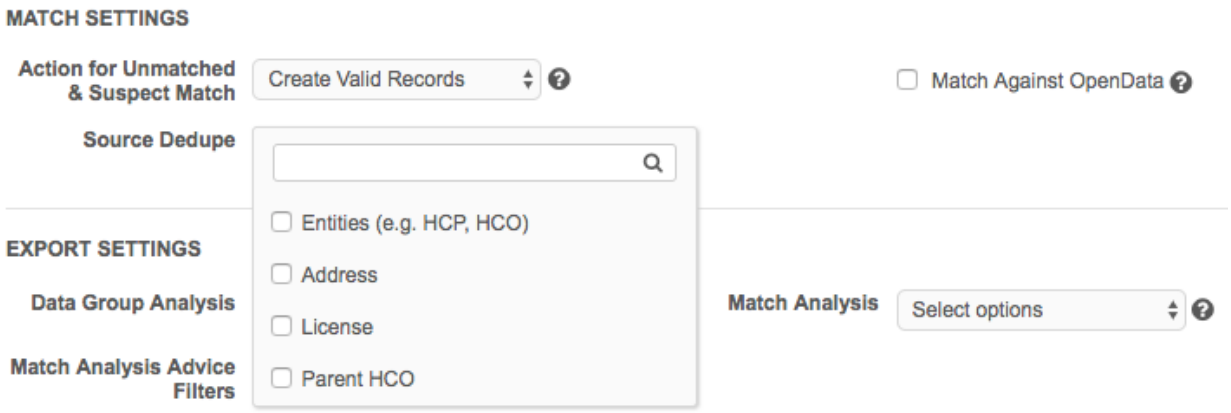
Result

When the data is loaded, Network first checks the custom keys for matches. In this example, the keys do not match, so Network uses the duplicate detection rules to determine if the objects are duplicates. The addresses are the same, so one address is loaded. In this example, the address with Source ID 7513B wins because it was the last row to be added. The phone number from the other address object is not included.

VID	Address Line 1	City	ZIP	Country	Phone	Custom Key
VID2A	123 Main Street	Salem	97310	United States	351-555-0000	SAP:Address:7513B SAP:Address:2215A

Deduplicate child objects

1. In the Admin console, click **System Interfaces > Source Subscriptions**.
2. Select an existing subscription, or create a new subscription.
3. In the **Settings** section, under **Match Settings**, click the **Source Dedupe** list.
4. Select the child objects that you want to deduplicate when the subscription runs.



Child object merging occurs after the HCP and HCO entities are matched together through source deduplication.

Job properties

When source subscriptions run, Network uses the following advanced properties for source deduplication:

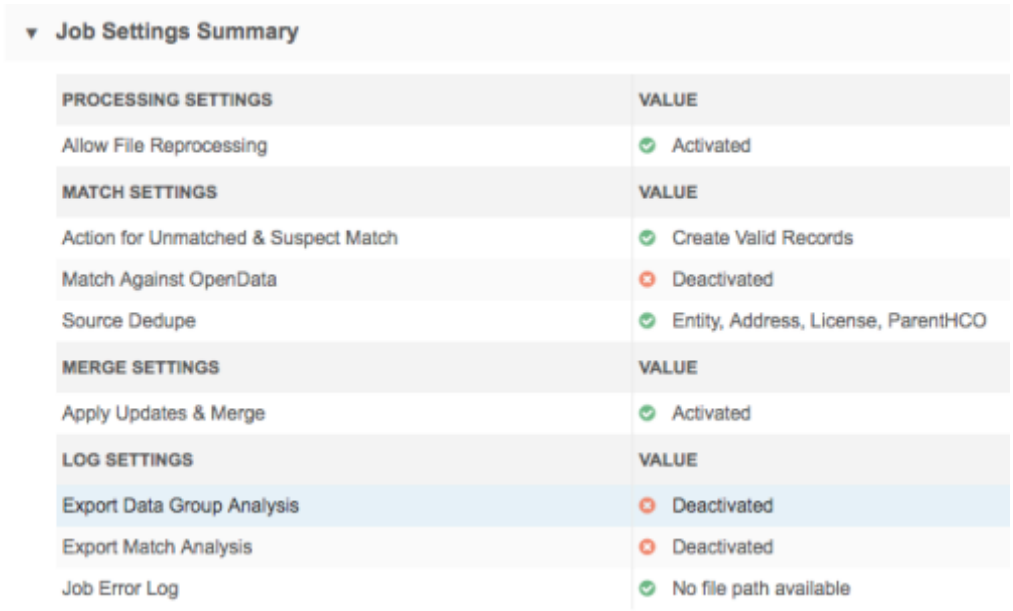
Entity source dedupe - `"job.match.dedup": "true"`. The value can be either *true* or *false*. The value is *false*, by default.

Child source dedupe - `"job.merge.childDedup": "Address,ParentHCO"`. The value can be any combination of *Address*, *License*, or *ParentHCO*. By default, there is no value.

Selecting the source deduplication options in the source subscription populates these job properties, but they can also be manually updated using **Advanced Mode**.

Job settings summary

To review the deduplication settings for the subscription, see **Source Dedupe** in the **Match Settings**. The list of objects that were selected for deduplication are listed. **Entity** refers to both HCPs and HCOs.



▼ Job Settings Summary

PROCESSING SETTINGS	VALUE
Allow File Reprocessing	Activated
MATCH SETTINGS	**VALUE**
Action for Unmatched & Suspect Match	Create Valid Records
Match Against OpenData	Deactivated
Source Dedupe	Entity, Address, License, ParentHCO
MERGE SETTINGS	**VALUE**
Apply Updates & Merge	Activated
LOG SETTINGS	**VALUE**
Export Data Group Analysis	Deactivated
Export Match Analysis	Deactivated
Job Error Log	No file path available

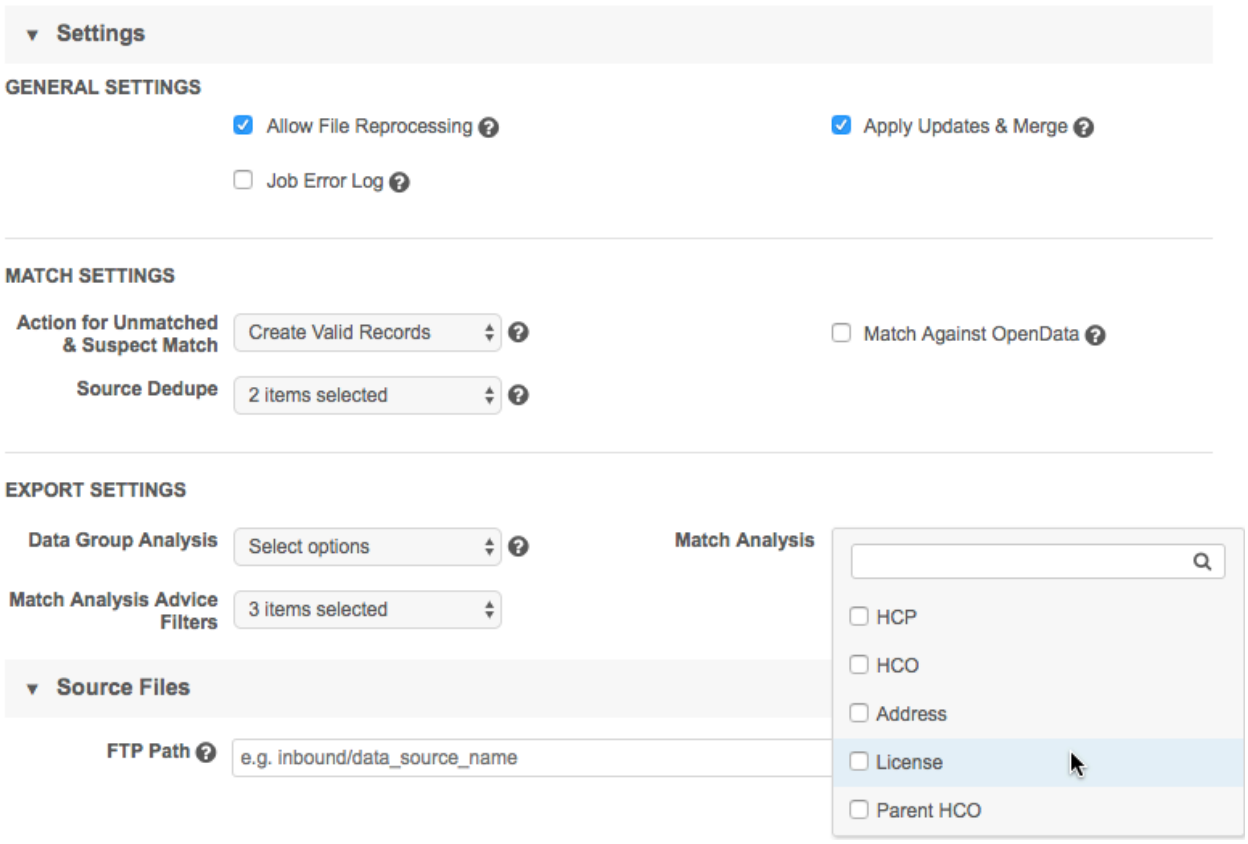
MATCH ANALYSIS LOGS

To help administrators and data managers track the child objects that are matched and merged during a source subscription job, they can now create match analysis logs for child objects. A separate log file is created for each child object. Child object match logs can be used independently of child object source deduplication.

To select the child object match logs to create:

1. In the Settings section, click **Apply Updates & Merge**. This must be selected for the child object logs to be created.
2. In the **Export Settings** section, click the **Match Analysis** list and select the child objects.

The logs are created when the source subscription job completes.



Note: Job performance will slow if match logs are exported for all child objects.

Match analysis logs are exported as a .csv file to the outbound folder in your FTP server. Each log provides details on which records matched and how it matched. It also includes details about both the incoming data and the data in the matching record.

The child object match analysis log contains the following columns of information:

- **Reason / Rule Name** - The method the match was found: N/A (Key Match), Field Match (duplicate detection rules), Network Entity ID (matched using the VID).
- **Advice**: ACT, ASK, or UNMATCHED. Child objects are only ACT or UNMATCHED.
- **Entity id** - The Network ID (VID) of the matching parent object.
- **Entity Type** - The entity type of the parent object; either HCP or HCO.
- **Source Address ID** - The Network ID (VID) or Archive ID of the source object.
- **Match Address VID** - The Network ID (VID) or Archive ID of the matching object.
- **Source Custom Key** - The custom keys of the source object.
- **Match Custom Key** - The custom keys of the matching object.

Example

Review the example to see the address match analysis log that is created when the following HCP and address data is loaded into Network.

HCP

The *HCP.csv* file contains the following information:

ID	first_name__v	last_name__v	npi_num__v	primary_country__v
2152	Chris	Woodson	9251950021	US
992	Christopher	Woodson	9251950021	US

When the subscription runs, Network matches these HCP records together using the NPI number

Address

The *address.csv* file contains the following information:

Address	ID	Address_ID	address_Line_1	locality__v	administrative_area__v	country__v	postal_code__v
1	2152	129889	15 York St	New York	US-NY	US	52152
2	2152	129889	15 York St	New York	US-NY	US	52152
3	2152	129890	62 York St	New York	US-NY	US	52152
4	2152	129891	62 York St	New York	US-NY	US	52152
5	992	129892	62 York St	New York	US-NY	US	52152
6	992	129892	62 York St	New York	US-NY	US	52152
7	992	129894	52 Water St	New York	US-NY	US	2150

Note: The Address column is added to help explain this example - it is not part of the .csv file.

Address match log

The exported match log tells you what existing address the incoming addresses matched on.

Rule Name	Advice	Entity Id	Entity Type	Source Id	Match Id	Source Custom Key	Match Custom Key	Source address_line_1__v	Match address_line_1__v	Source administrative_area__v	Match administrative_area__v	Source country__v	Match country__v
N/A	UNMATCHED	930688713210265631	HCP	930688713209020448		test1:ADDRESS:129889		15 York St		US-NY		US	
N/A	UNMATCHED	930688713210265631	HCP	930688713210331168		test1:ADDRESS:129890		62 York St		US-NY		US	
Field Match	ACT	930688713210265631	HCP	930688713210396703	930688713210331168	test1:ADDRESS:129891	test1:ADDRESS:129890	62 York St	62 York St	US-NY	US-NY	US	US
Field Match	ACT	930688713210265631	HCP	930688713210396704	930688713210331168	test1:ADDRESS:129892	test1:ADDRESS:129890	62 York St	62 York St	US-NY	US-NY	US	US
Field Match	ACT	930688713210265631	HCP	930688713210396705	930688713210331168	test1:ADDRESS:129893	test1:ADDRESS:129890	62 York St	62 York St	US-NY	US-NY	US	US
N/A	UNMATCHED	930688713210265631	HCP	930688713210396706		test1:ADDRESS:129894		52 Water St		US-NY		US	

- Address 1 and 2 matched using key match because the custom keys are identical. In the match log, one entry displays. The **Advice** column displays `UNMATCHED` because the record did not match an existing record in Network. A new address record is created in Network.

  If addresses are matched using key matching the match log shows one entry; the new address.

- Address 3 was processed next. There were no existing records in Network for this address to match, so the match log shows it as `UNMATCHED`; a new record is created in Network.
- Addresses 4, 5, and 6 were processed next and they matched to Address 3 using duplicate detection rules. The match log advises that these records `ACT` matched and displays Address 3's custom key as the matching key in the **Match Custom Key** column.
- Address 7 did not match any existing records in Network so the match log advises that it was `UNMATCHED`. A new record for the address is created in Network.

Log file names

When child object match logs are exported, they are zipped together in one file.

File Name: `<System>-CHILD-MATCH-ANALYSIS-<Date and Time Stamp>-job-<Job ID>.zip`

Example: `SAP-CHILD-MATCH-ANALYSIS-2017-05-15T09-29-0700-job-5001.zip`

Extract the file to view each child object match log.

File Name: `<System>-<ChildObjectName>-MATCH-ANALYSIS-<Date and Time Stamp>-job-<Job ID>.csv`

Example: `SAP-ADDRESS-MATCH-ANALYSIS-2017-05-15T09-29-0700-job-5001.csv`

Child object match logs are deleted from the FTP folder after three days.

Advanced job property

When source subscriptions run, Network uses the following advanced property for match analysis logs:

`"Job.match.export": "HCP,HCO,Address,License,ParentHCO".`

The value can be any combination of *HCP*, *HCO*, *Address*, *License*, or *ParentHCO*. By default, there is no value.

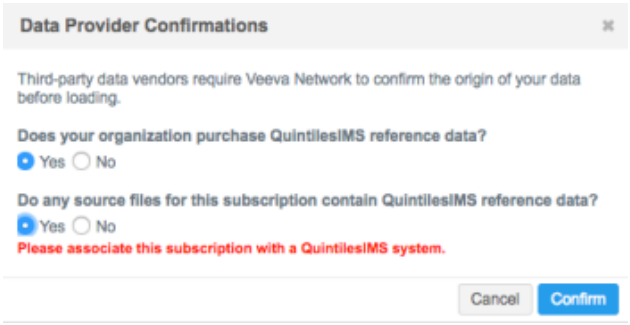
Selecting the match analysis log options in the source subscription populate this job property, but it can also be manually updated using **Advanced Mode**.

DATA PROVIDER CONFIRMATION

When new source subscriptions are created, a new dialog require answers to questions about the origin of the data. This provides an additional level of security to ensure the safety and security of data for third party providers.

When an administrator saves a new subscription, a dialog displays the required questions. Administrators must select either **Yes** or **No** for each question.

- **Does your organization purchase QuintilesIMS reference data?**
  - If you answer **No** to this question, click **Confirm**.
  - If you answer **Yes** to this question, another question displays.
- **Do any source files for this subscription contain QuintilesIMS reference data?**
  - Select **Yes** or **No** and then click **Confirm**.

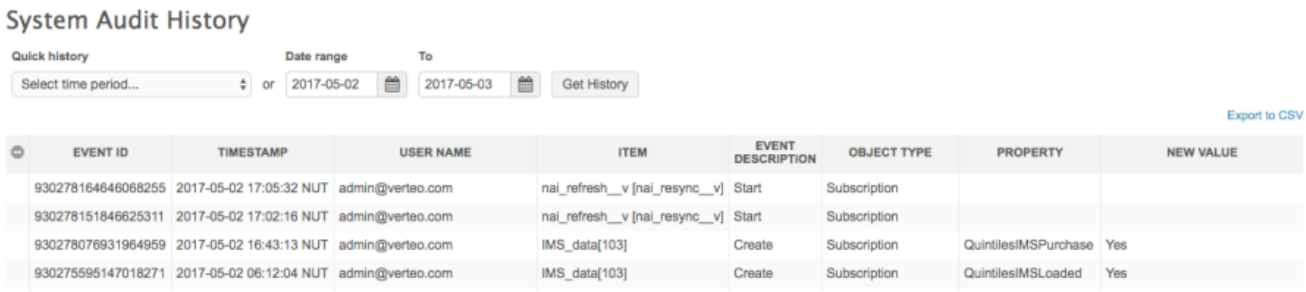


Audit

The answers to the questions are auditable and are logged in the **System Audit History**. The audit information includes:

- Time stamp
- User
- Subscription name
- Question ID
- Response (Yes, No)

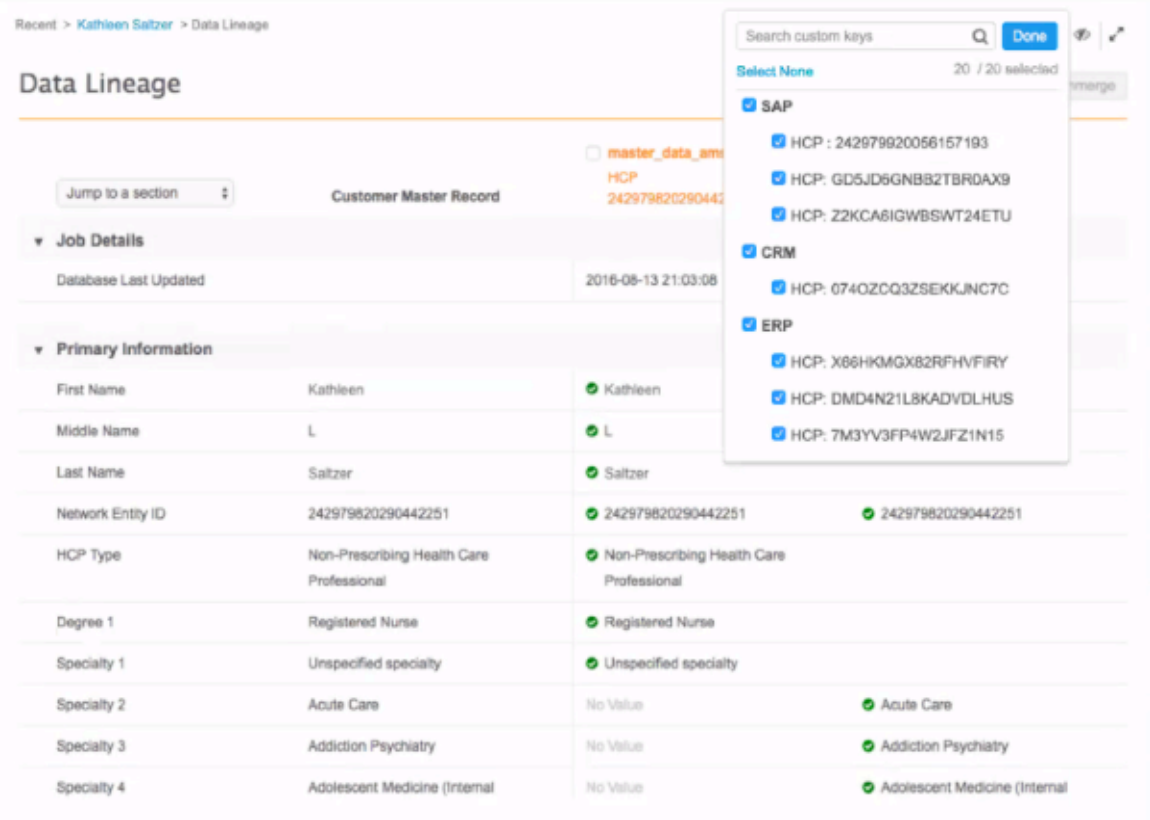
To view the audit information, in the Admin console, click **Logs > System Audit History**.



Data lineage

FILTERING BY SOURCE

Users can now select the data lineage views by source system. Previously, users could only select individual custom keys. This enhancement enables users to easily select all of the custom keys for each source.



To filter the data lineage view:

1. On any profile, click **Data Lineage** from the left navigation.
2. On the Data Lineage page, click the **Select Sources** list.

   The list is sorted by source.

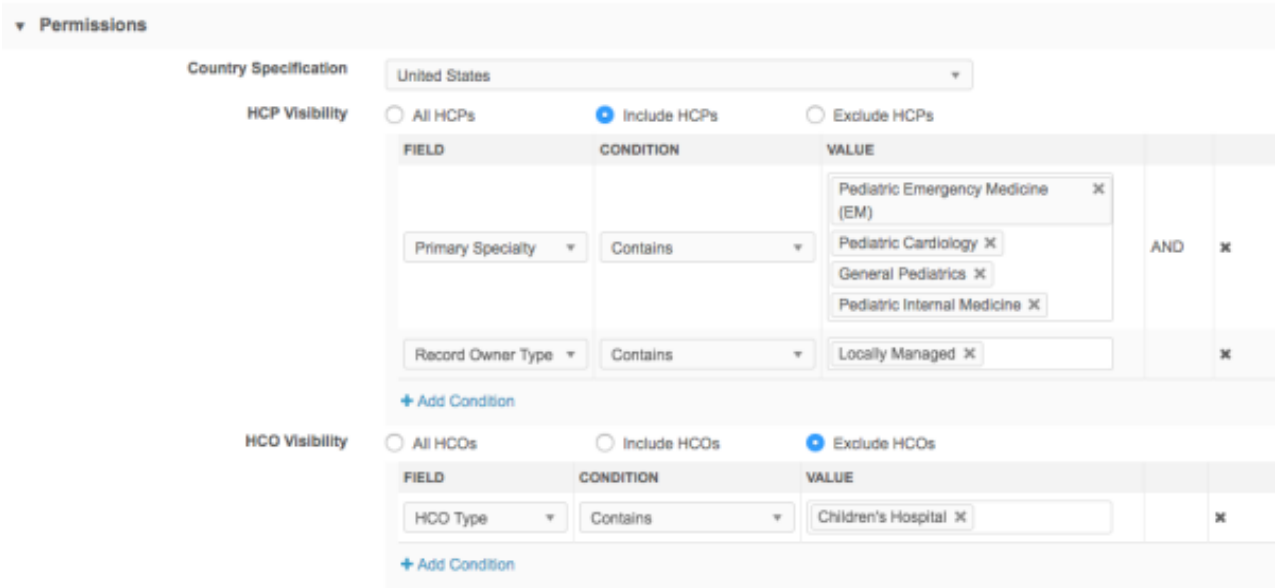
3. Choose either to view the data lineage by source (includes all custom keys for the source) or by selected custom keys.

Data visibility profiles

FILTERING RECORDS

Administrators now have more flexibility for filtering the records that users can access in the Network UI and the API. Data visibility profiles contain new filters so that HCP and HCO records are restricted from search, retrieval, reports, and viewing profiles. This is helpful for restricting records from users when products should be confined to specific HCP prescribers. For example, if you are marketing or selling a drug that could be dangerous for children, you can restrict users from searching or viewing HCP prescribers that specialize in pediatrics. It also helps to provide more relevant search results because users will only see the records that they have access to.

These filters apply to entities (HCPs and HCOs) and any related parent HCOs.



The filters do not apply to data change requests. To restrict data stewards from viewing tasks for certain HCO types or HCP types, use inbox task groups. For more information, see the *Veeva Network Online Help*.

Filter options

Filters can be applied for HCPs and HCOs.

HCP's are filtered by the following fields:

- **Record Owner Name** - The actual name of the record owner: **OpenData**, **Local**, or the third party data provider's name. This is a new field that is now available in the data model and can be used for Network reporting after the Network 17R2.0 release.
- **Record Owner Type** - The type of record: **OpenData**, **Locally Managed,** or **Third Party**. This is a new field that is now available in the data model and can be used for Network reporting after the Network 17R2.0 release.
- **HCP Type** - Any HCP type that is defined in the data model.
- **Primary Specialty** - Any specialty (`specialty_1__v`) that is defined in the data model.
- **Specialty 1 or 2** - Any specialty (`specialty_1__v` or `specialty_2__v`) that is defined in the data model.

HCO's are filtered by the following fields:

- **Record Owner Name** - The actual name of the record owner: **OpenData**, **Local**, or the third party data provider's name. This is a new field that is now available in the data model and can be used for Network reporting after the Network 17R2.0 release.
- **Record Owner Type** - The type of record: **OpenData**, **Locally Managed**, or **Third Party**. This is a new field that is now available in the data model and can be used for Network reporting after the Network 17R2.0 release.
- **HCO Type** - Any HCO type that is defined in the data model.

Filter records using data visibility profiles

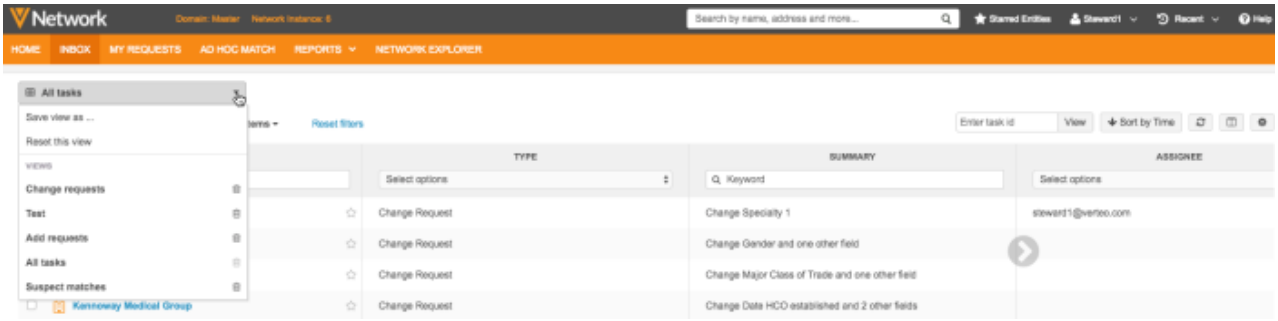
To add record filters to a data visibility profile:

1. In the Admin console, click **Users > Data Visibility Profile**.
2. Select a data visibility profile from the list.
3. Click **Edit**.
4. In the **Permissions** section, select the country that these filters apply to.
5. For **HCP Visibility** and **HCO Visibility**, select an option:
    - **All HCP** or **All HCO** - Do not filter. All records are visible.
    - **Include HCP** or **Include HCO** - Choose HCPs or HCOs that should be visible for this data visibility profile.
    - **Exclude HCP** or **Exclude HCO** - Choose HCPs or HCOs that this data visibility profile should not have visibility to.
6. If you chose **Select HCP** or **Exclude HCP**, click **+ Add Condition**.
7. Select the **Field**, **Condition**, and **Value** that you want to filter by.
8. **Save** your changes.

Inbox

SAVING VIEWS

Data stewards, data managers, and administrators can now save inbox views. Saving views enables these users to organize their inbox so that they can more easily manage different types of tasks in their inbox. For example, data stewards and data managers can create separate views for change requests, add requests, and suspect matches. They can toggle between the views depending on the type of task that they're working on. Administrators can create views to organize tasks of different data loading jobs.



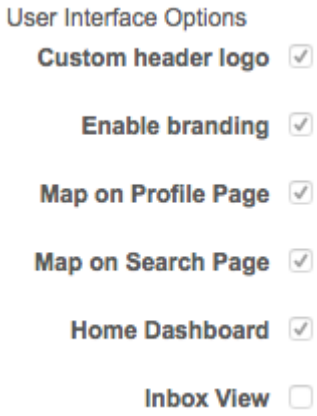
Saved inbox views apply to each user; they cannot be shared among users.

Enabling this feature

This feature is enabled by default for new customers. Existing customers can enable the feature for their Network instance.

Administrators can enable this feature in their Network instance.

1. In the Admin console, click **Settings > General Settings**.
2. Click **Edit**.
3. In the **User Interface Options** section, select **Inbox View**.
4. **Save** your changes.



Now, when data stewards, data managers, and administrators log into this Network instance, they can create inbox views. If users do not create views, the default inbox behavior does not change.

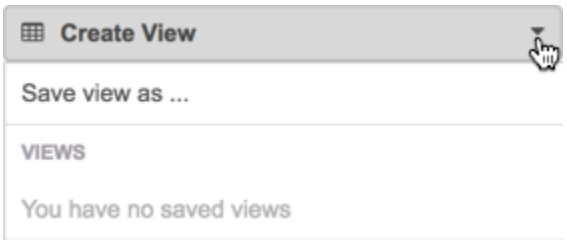
Creating inbox views

Any change that you make to the inbox configuration can be saved as a view. This includes filtering chosen columns, resizing those columns, sorting, number of records displayed, and so on. Users can create a maximum of fifty views.

Note: When you start creating views, the default Network inbox behavior is no longer available to return to. The inbox will default to the view that you were last using when you logged out of Network.

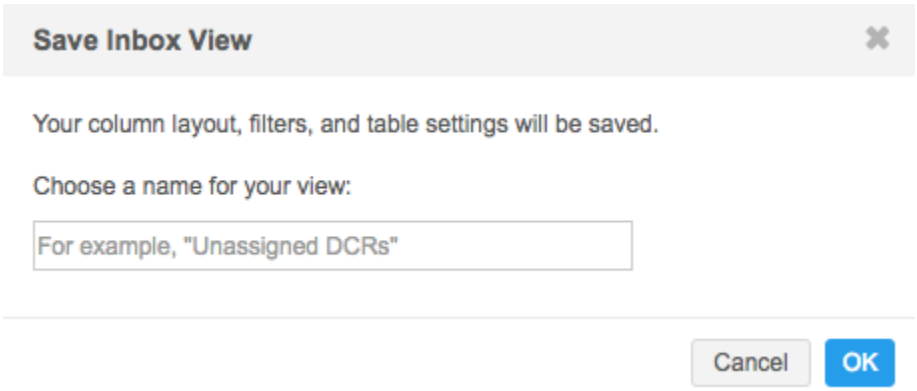
To create a new view:

1. Customize the view with the data and configuration that you want to save.
2. In the top left corner of the inbox, click **Create view > Save view as ...**.

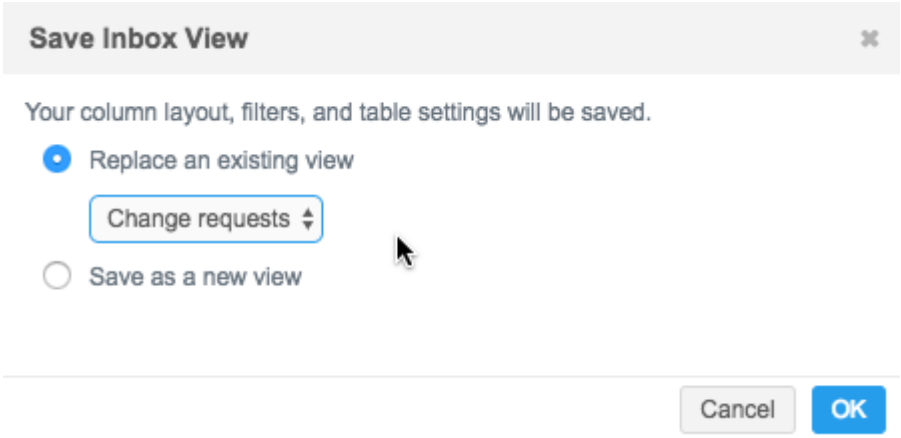


3. On the **Save Inbox View** dialog box, type a name for the view.

   The name cannot be longer than 80 characters.

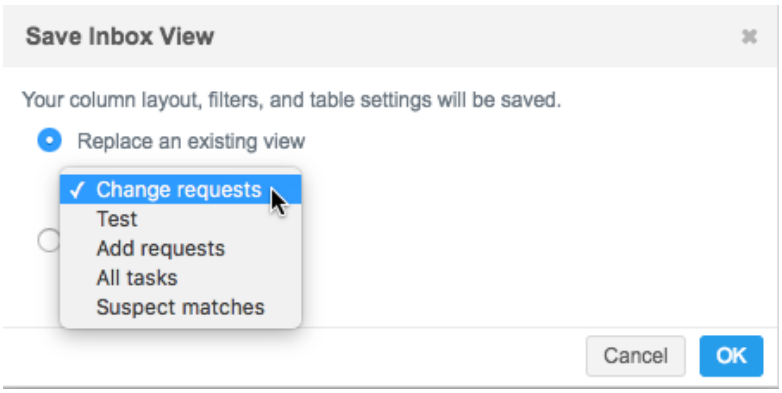


If you have previously created a view, the **Save Inbox View** dialog box is different.



Select the appropriate option.

- **Replace an existing view** - Overwrite an existing view with these changes. Select the view from the list.



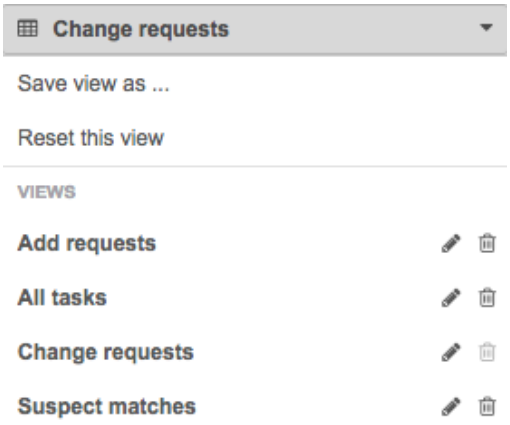
- **Save as a new view** - Create a view with a new name.

4. Click **OK**.

When a view is saved, the inbox displays the view. If users navigate away from the inbox and then return, the last view that they used displays.

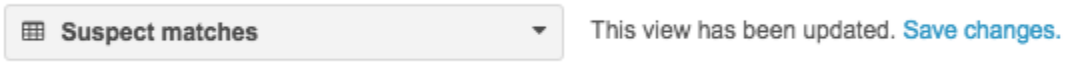
Select saved views

Users can switch between views by expanding the current view and selecting a new view from the list. All views are listed alphabetically.



Update views

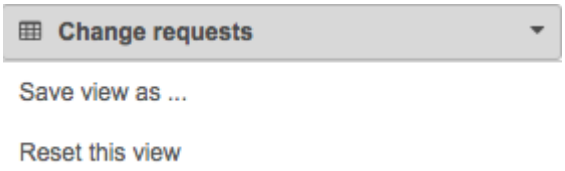
When users make changes to a view (for example, sorting or filtering), a message displays beside the view name to remind users to save the changes. Click **Save changes**.



If the view changes are not saved, the changes are persisted for the user's session. Users can navigate away from the inbox, but still see unsaved changes when they return to the inbox. If users log out of Network and log in again, unsaved changes to the view are lost.

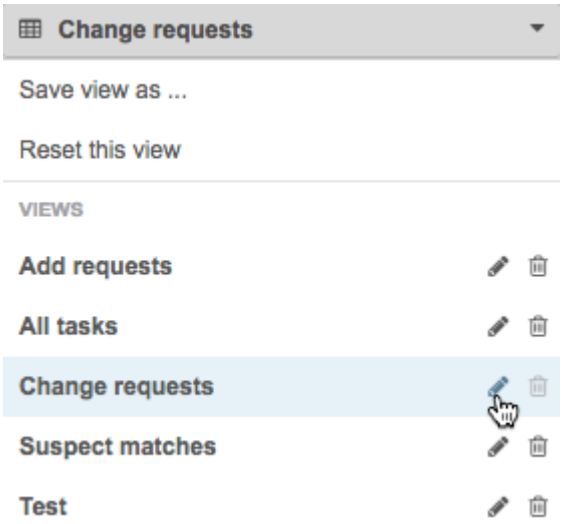
Reset views

Users can make changes to a view and then reset the view to return to the saved configuration. For example, if data stewards sort or filter columns, but don't want to save the change, they can click **Reset this view** to revert the changes.

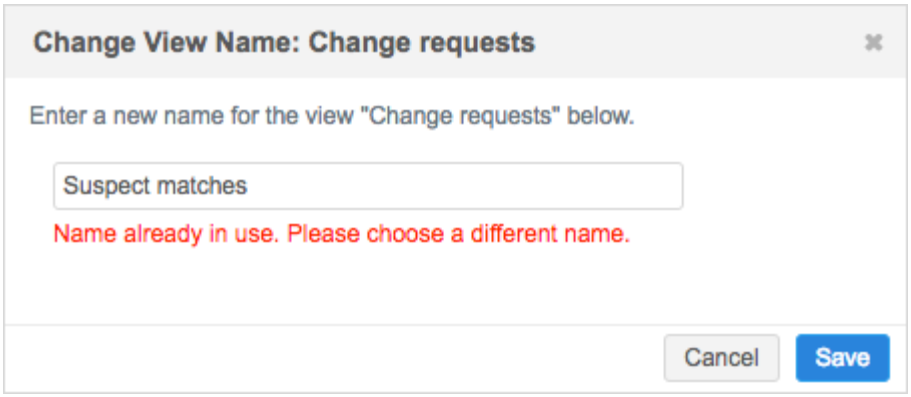


Edit view names

Users can edit view names to correct a mistake or adjust the name to reflect changes. To edit the name, in the list, click the **Pencil** icon.

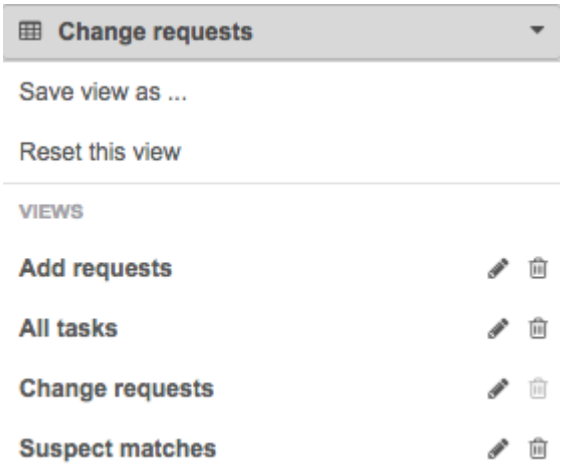


Edit the name and **Save** your changes. Network validates that an existing view does not have the same name.



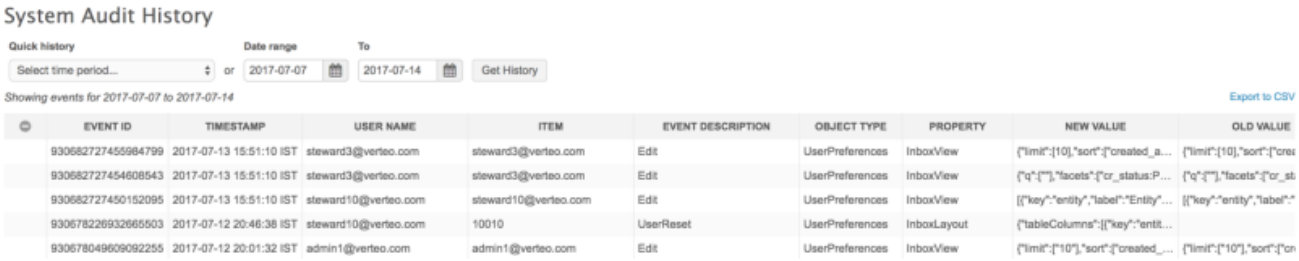
Delete views

When views are no longer required, they can be deleted by selecting the **Delete** icon in the list. The **Delete** icon for the current view is dimmed and cannot be deleted. This ensures that the inbox always has one saved view.



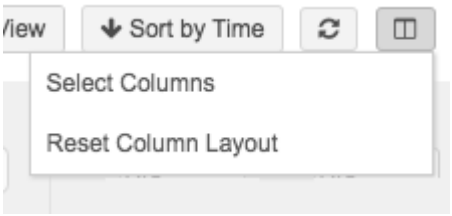
Auditing

Network tracks views that are created, updated, and deleted and records the actions. Administrators can see the audit logs by navigating to **Logs > System Audit History**.



SELECTING AND RESETTING COLUMNS

The options for selecting and resetting columns are now easily accessible on the inbox view. Data stewards, data managers, and administrators can click the new **Column Options** button to quickly change their columns.



Previously, the column options were in **More Options**.

The behavior of the column options has not changed. For more information about these options, see the *Veeva Network Online Help*.

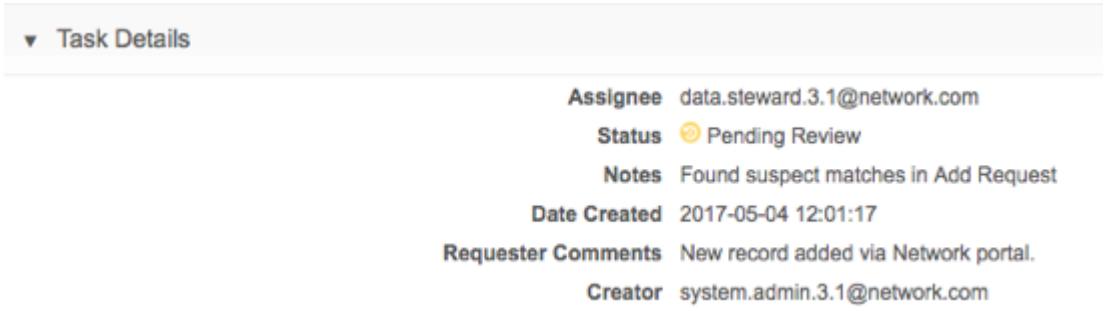
TASK DETAILS

Suspect match tasks now include details about how the task was created - through a data loading job; manually, using the **Find Suspect Match** action through the Profile; or, through an add request. This information is useful for triaging tasks.

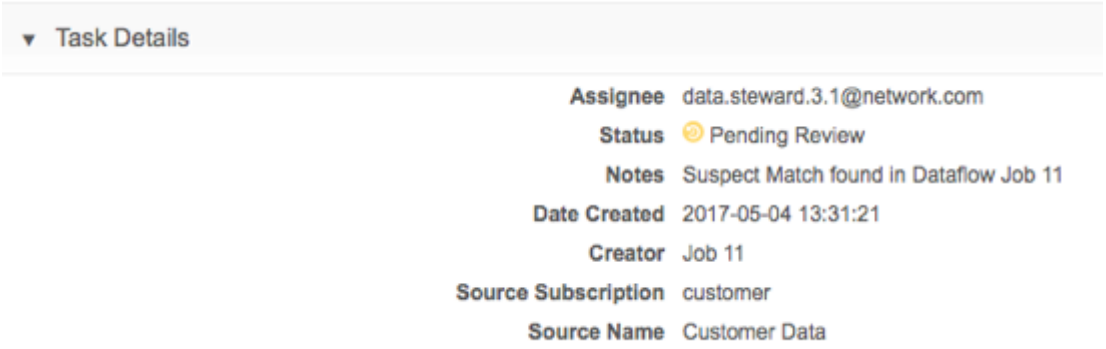
To view the information, see the **Task Details** section at the bottom of the suspect match task.

The **Creator** details depend on how the suspect match originated:

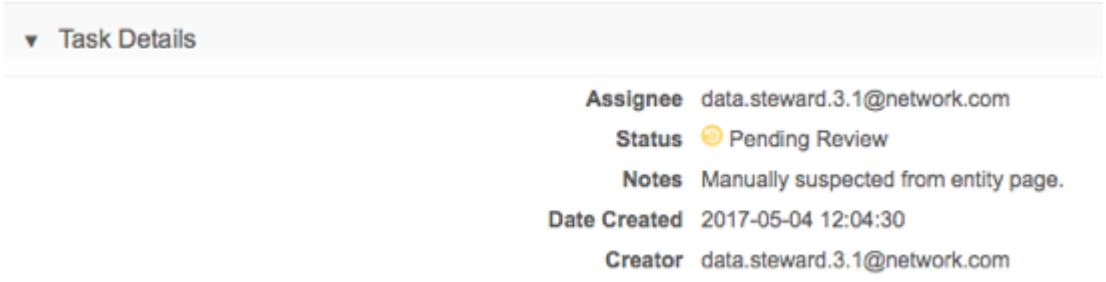
- **Add request** - The user that created the request.



- **Data loading job** - The job ID. For example, `Job 11`.



- **Manually** - The user who initiated the task using the **Find Suspect Match** action on the Profile. Typically, a data steward creates these tasks.



Network address inheritance

REFRESHING CHILD ADDRESSES

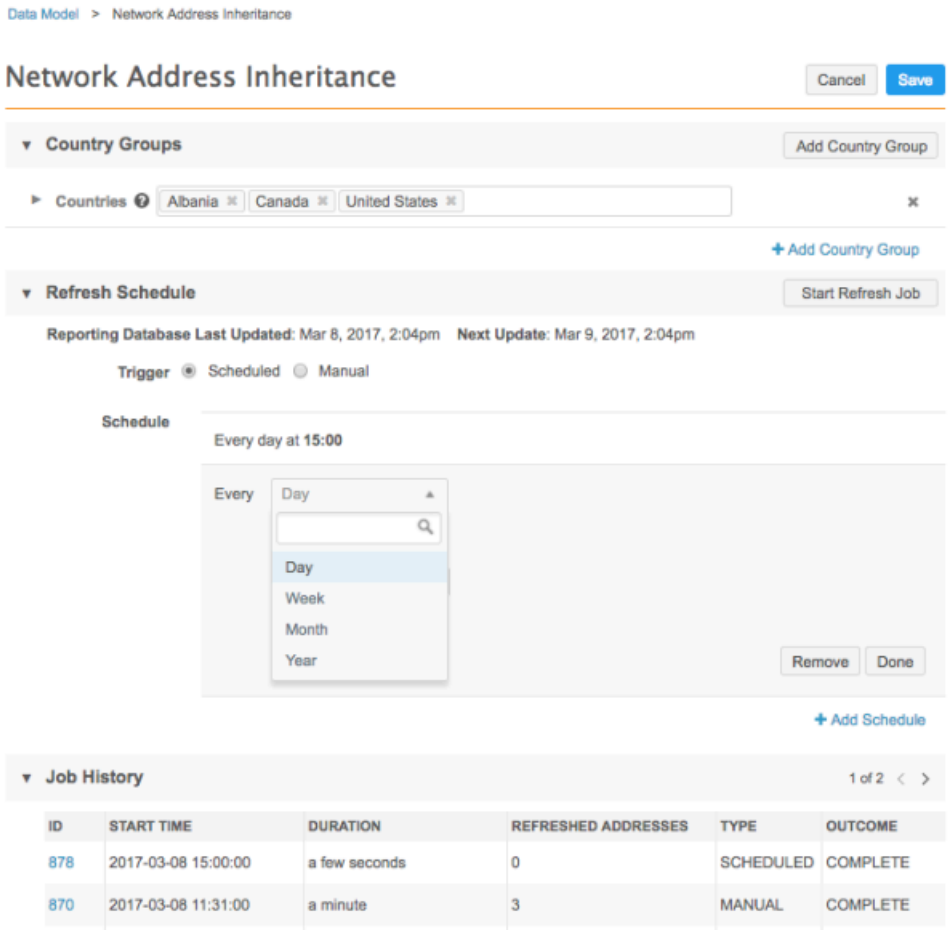
If you are using the Network Address Inheritance feature, address information can become out of sync between a child address and its parent as data is updated and changed by DCR processing and subscription updates. Network Address Inheritance now contains a maintenance feature that identifies out-of-sync child addresses and syncs them to the parent address again automatically.

Previously, child addresses would only sync again if the record containing the child address was edited by a user. This maintenance feature ensures that your data quality is preserved using scheduled updates.

This enhancement is available by default if Network Address Inheritance is enabled in your Network instance. Network reporting must be available in your instance for this feature to work; reporting must run so that data is refreshed.

Scheduling updates to refresh addresses

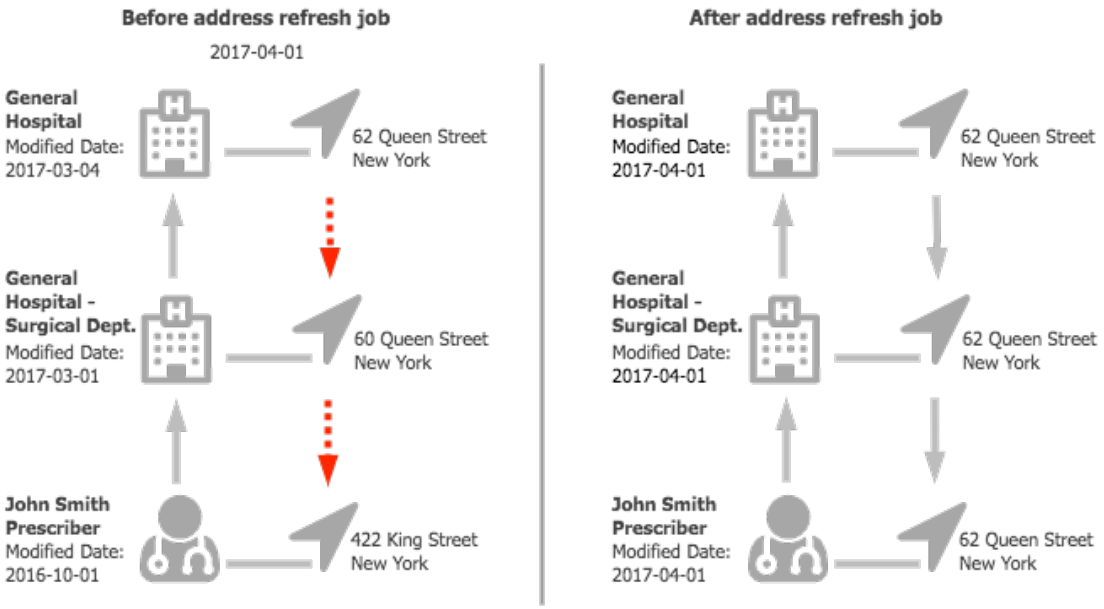
On the **Data Model > Network Address Inheritance** page, administrators and data managers can schedule multiple jobs on daily, weekly, monthly, or yearly schedules.



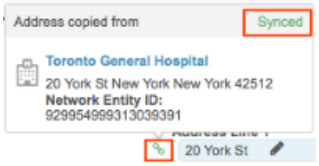
To manually update out of sync child addresses, click **Start Refresh Job** to start the maintenance job.

During the job, Network updates child addresses that are out of date with their synced parent address. The query looks to see if the parent address has been updated more recently than the child address. Network Address Inheritance logic runs on the child address to ensure that it's updated and in sync again. If new addresses are found on the parent record, the new address is copied to the child record.

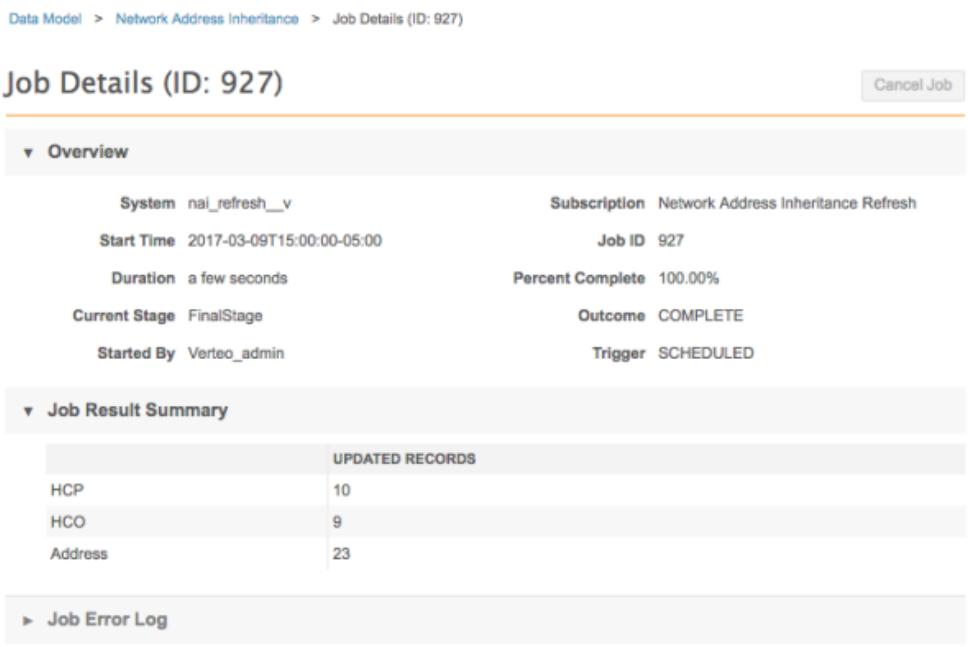
Review the following diagram to see how Network determines if an address is out-of-sync.



This maintenance job only considers child addresses that have a `parent_address_status_v` field with the following values: *Synced*, *Re-sync*, or *Disqualified*. This field value can be found on the address in the profile.



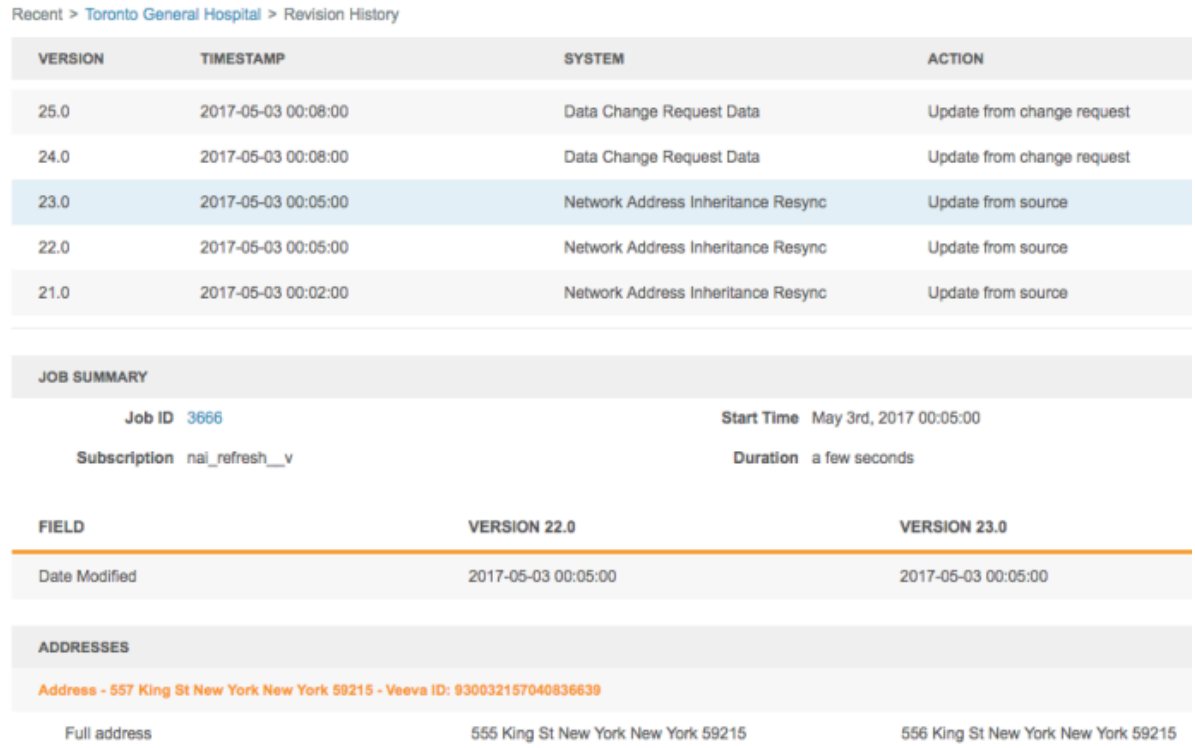
When the job completes, in the **Job History** section click the **ID** link to open the Job Details page and view summary information about the job.



Revision history

When an address is changed to sync to its parent address, the change is tracked in the **Revision History**.

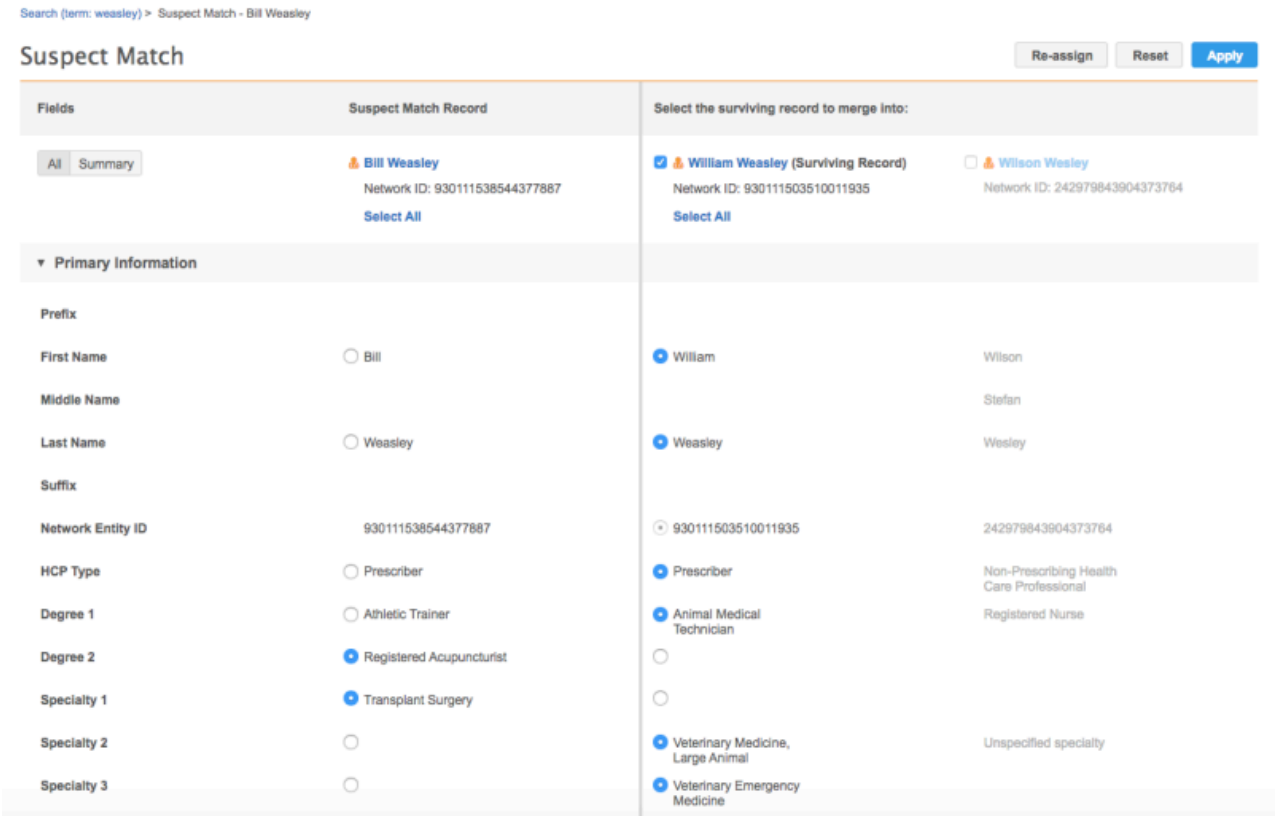
If a change is made to the record, Network business rules might run; for example, primary affiliation, primary address, or address ordinal sorting. All of these record changes are also included in the Revision History.



Suspect match

SELECTING SURVIVING FIELDS

Data stewards and data managers can now select individual fields to retain on the surviving record of a suspect match. This ensures that the surviving record of a merge has the most accurate, complete, and current information. Previously, data stewards and data managers could only select the record; survivorship of field values was determined in the background based on source ranking. This enhancement also includes usability improvements that make it easier to distinguish the winning and losing record of the merge.



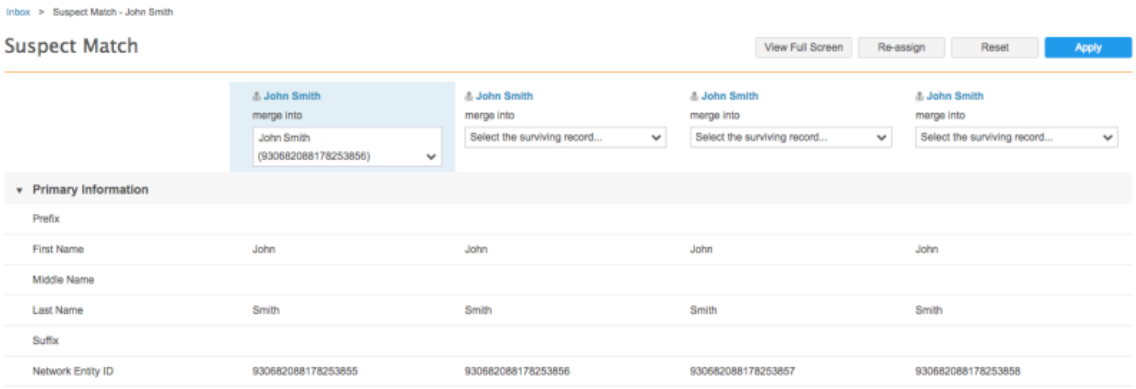
Data stewards and data managers cannot select individual fields in the following situations:

- The incoming suspect match record does not have a Network ID (VID).

  This occurs when the Create Unverified option is not enabled in the General Settings; a DCR is created, but it is not considered a record because it does not contain a VID. In the suspect match task, a surviving record can be selected, which creates a change request. Data stewards and data managers can accept or reject fields from the incoming record on the change request, as usual.

- The suspect match task originated from source deduplication.

  Individual fields cannot be selected, but the records can be merged using the Network ID (VID).

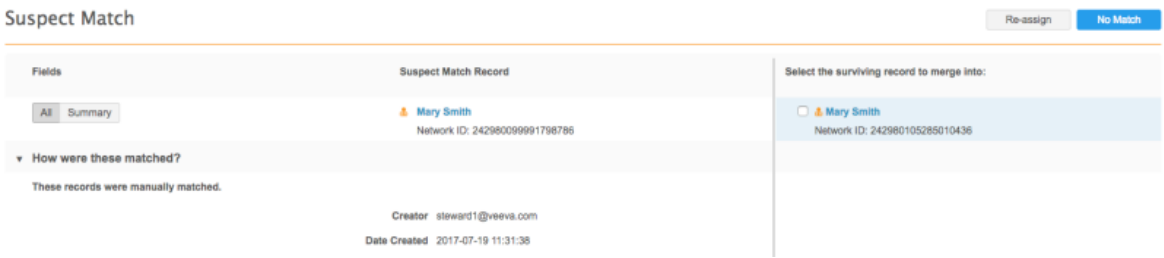


Usability enhancements

Suspect match tasks are updated to help the data stewards and data managers more easily process tasks.

The following enhancements have been introduced:

- A line separates the suspect match record and potential surviving records (all the records that the suspect match record matched against).
- Labels are added to the separated sections to define the suspect match record and the potential surviving records.
- The Network Entity ID (VID) displays below the record name.
- The reasons why the records matched with the suspect match records display. For add requests and data loads, the match rules are identified. For suspect matches created using **Find Suspect Match**, the message identifies that the task was manually created and displays the creator and date of the task.

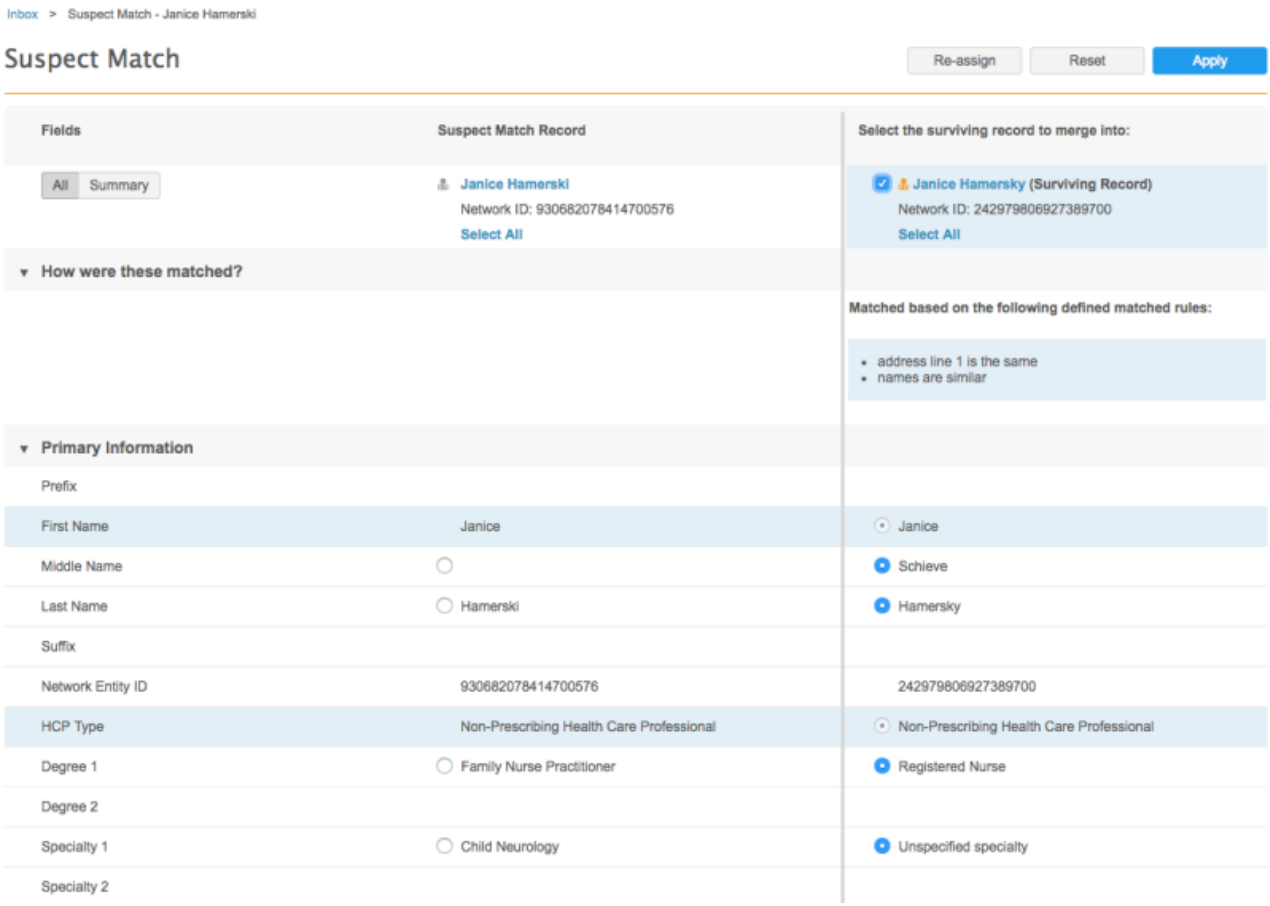


Selecting fields

When data stewards and data managers open a suspect match task from the inbox, the suspect match record and any matching records are clearly defined and separated. After data stewards or data managers select the surviving record of the merge, they can select individual fields to be retained on the surviving record. Their selections can overrule the survivorship rules defined in Network.

Suspect match field behavior:

- When the surviving record is selected, records that were not selected as a match are dimmed and cannot be selected. Only values from the suspect match (source record) and the surviving record (target record) can be selected.
- The fields on the surviving record are selected by default. If the suspect match record has a field with a value and the surviving record does not, the field is selected on the suspect match record.
- If the field values are identical between the suspect match record and surviving record, the values on the surviving record are selected and no selection is required; the value for the surviving record is retained



Child object considerations

Child object fields (addresses, licenses, and Parent HCOs) cannot be selected. If the child objects are exactly the same between the suspect match record and the surviving record, the objects are merged. If the child objects are different, they are both included on the surviving record.

Mastered record considerations

If the suspect match record matches with a mastered surviving record (either Veeva OpenData or third party master) the values of the mastered record are always retained. Only the surviving values for local (gray) fields can be selected.

Locked fields

Some fields on records must always be retained, for example, `created_date__v`, `record_state__v`, `is_properprietary__v` and so on. These fields cannot be selected. Locked fields are typically the fields on the Profile page that contain the **Locked** icon.

Data validation rules

Data validation rules ensure that data is complete and accurate before record changes are processed for add or change requests. For suspect match merges, data validation rules run when two records are merged and field values have been selected from the suspect match record. In this situation, merging the records includes a change request for the updated values, so the data validation rules will run. If a data validation rule fails, the change request task will be listed in the inbox for a data steward to review and address.

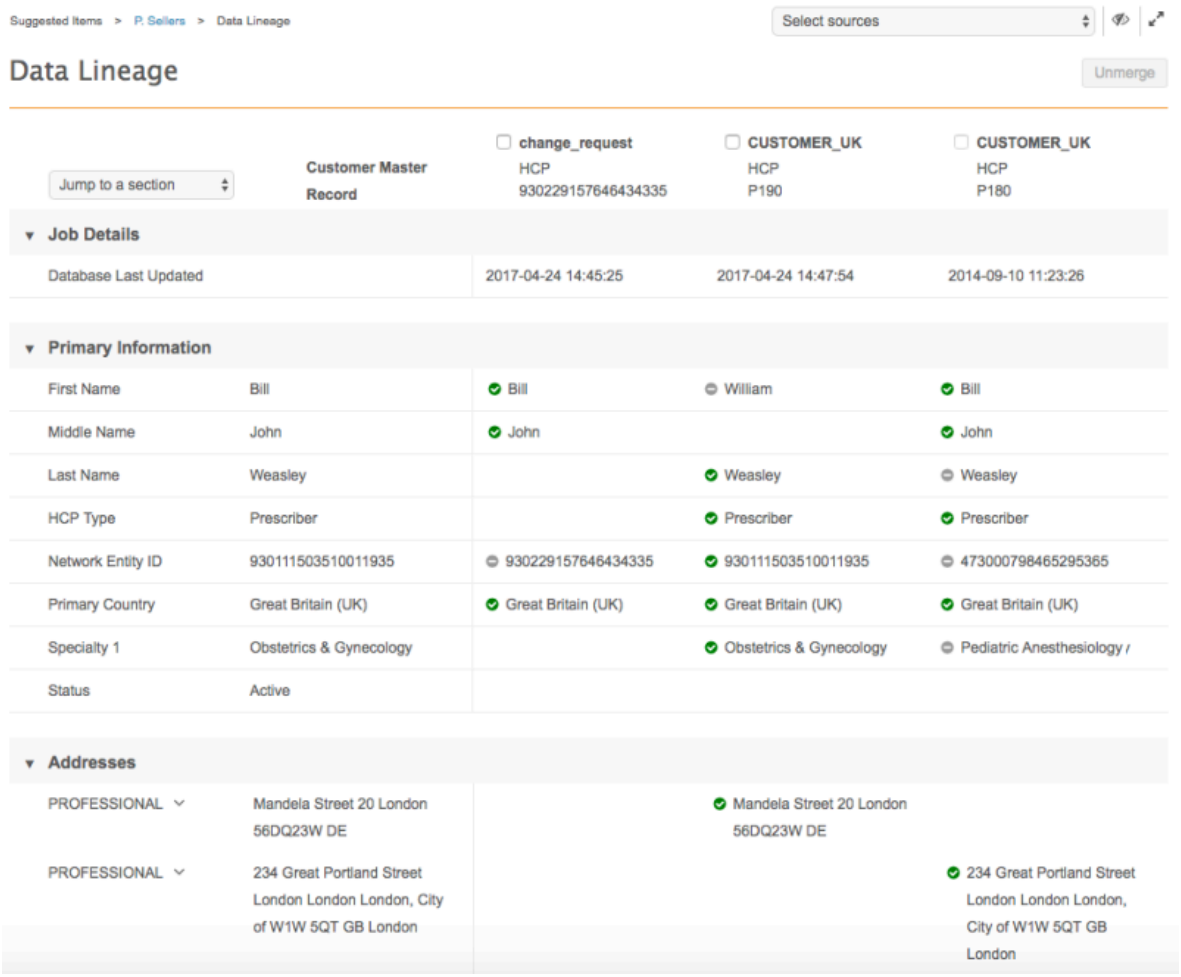
If two records are merged and no field values have been selected from the suspect match record, data validation rules do not run. The merge request does not contain changes, so data validation is not required.

Data lineage

Selecting individual fields to retain on the surviving merge record can change the data lineage for the surviving record.

When data stewards or data managers change the surviving record by picking field values from the suspect match record, a change request is applied to the surviving record. The values from the losing record display as a **change_request** in the data lineage. This ensures that the selected values are not reverted to the previous values of the surviving record when the surviving record is loaded through a source subscription. A change request is higher than a source system in the source rankings.

If no field values on the surviving record were changed, then no change request is applied.

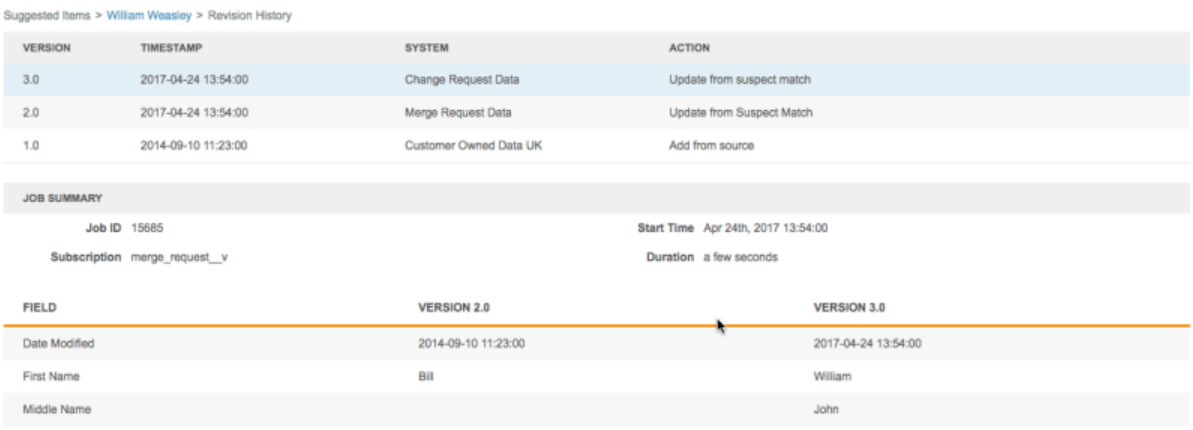


Revision history

The Revision History for the surviving record will show two record versions if field values are picked from the suspect match record:

- The update from the merge request
- The update from the change request

  Field values that were selected from the suspect match record display in the Revision History.

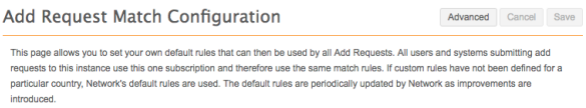


Match

The button name for the advanced match options in Match features has been renamed to **Advanced**. Previously, the button name was **Advanced Mode**. The button is renamed to align with the **Advanced** button in source subscriptions that is used to access the XML.

This change affects the following match features in the **System Interfaces** menu:

- Ad Hoc Match Configuration
- Match Default Configuration
- Add Request Match Configuration

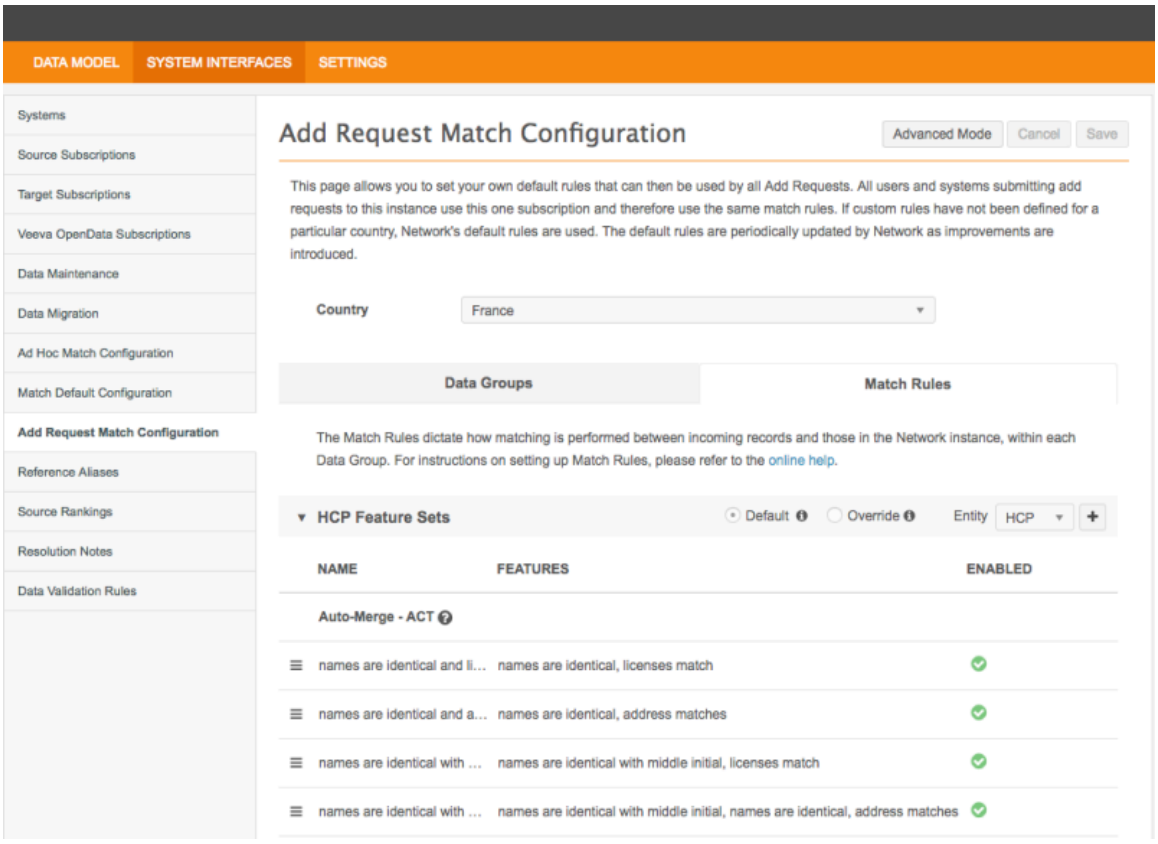


ADD REQUEST MATCH RULES

Add request behavior is determined by the change request subscription, `change_request__v`. This subscription can now be accessed in the Network user interface so that administrators can define custom match rules for add requests.

All add requests submitted to your Network instance use the default Network match rules unless custom match rules are defined for a particular country. This applies to add requests from any system or user in your Network instance.

This feature is enabled by default.



Defining match rules

To customize match rules for add requests:

1. In the Admin console, click **System Interfaces > Add Request Match Configuration**.
2. In the **Country** drop down list, select the country for customizing the match configuration.
3. The default Network data groups and match rules are applied for each country. Change the match rules or add new rules.

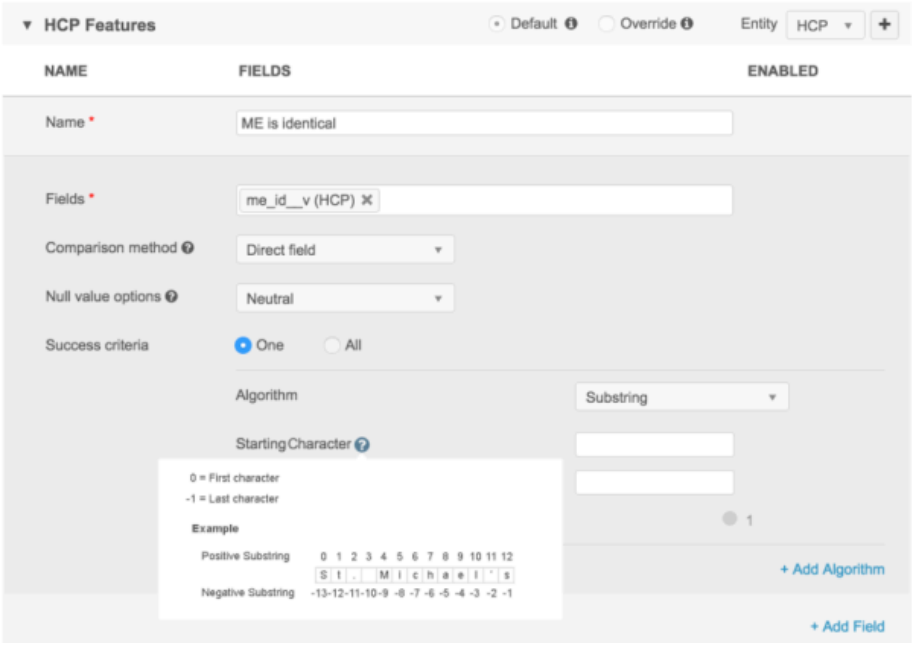
   Note: If you have previously customized match rules for the country with the help of Veeva Professional Services, those customizations will display.

4. To edit data groups or match rules using XML, click **Advanced Mode**.
5. **Save** your changes.

All add requests submitted to your Network instance for this country will now use the customized match configuration. Add requests that are sent to a Veeva OpenData instance will use the match rules in that instance which may differ from your own.

SUBSTRING ALGORITHM TOOLTIP

In the Match Rules Basic mode, HCP Features supports using the Substring algorithm with negative values. To help users define negative substrings, a tooltip has been added to the **Starting Character** field.



MONGE ELKAN ALGORITHM

In the Match Rules, sub algorithms can now be embedded into the Monge Elkan algorithm. This applies to any match configuration in the Network instance.

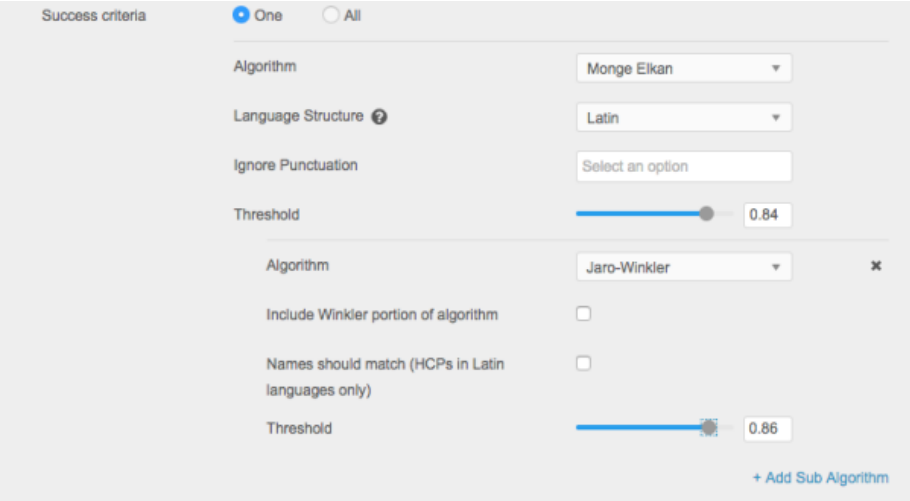
The Monge Elkan algorithm is a hybrid string comparison. It breaks the strings into tokens and then compares the tokens. This default comparison can be overridden by using a sub algorithm, such as the Jaro Winkler or the n-gram comparisons.

Administrators can now use the Monge Elkan comparison in **Basic** mode in their match configurations. Previously, this algorithm could only be successfully configured in **Advanced Mode**.

To embed a sub algorithm:

1. Open your match configuration.
2. Click the **Match Rules** tab and scroll to the **HCP Features** section.
3. Using an existing feature, or a new feature, in the **Success criteria** section, choose **Monge Elkan** from the **Algorithm** list and define the settings.
4. Click **+ Add Sub Algorithm**.
5. Select the algorithm that you want to embed and define the settings. Additional algorithms can be embedded.
6. Click **Done**.

7. **Save** your changes.

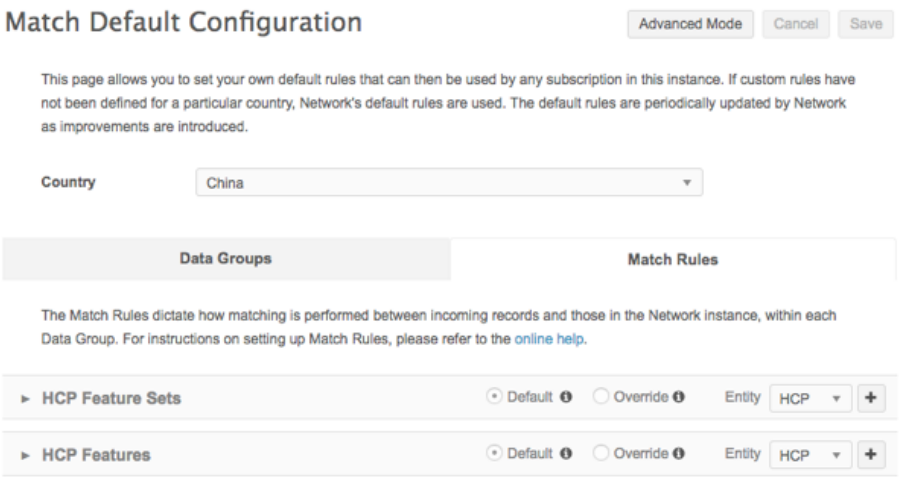


PINYIN JARO ALGORITHM

The Pinyin Jaro algorithm compares Chinese character strings using Hanyu Pinyin as a measure of character equivalence and the Jaro algorithm for overall string similarity. Administrators can now use the Pinyin Jaro comparison in **Basic** mode in their match configurations. Previously, this algorithm could only be successfully configured in **Advanced Mode**.

MATCH CONFIGURATION FOR CHINA SUPPORTED IN BASIC MODE

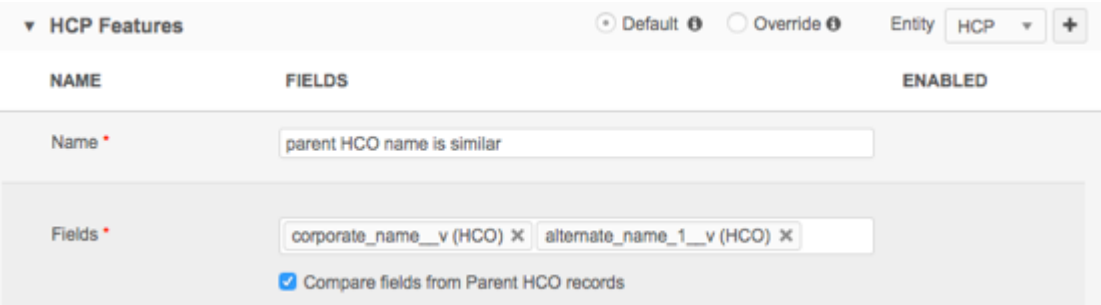
The default match rules for China use a particular configuration, so they previously had to be managed in **Advanced Mode**. Now, these match rules can be viewed and managed in **Basic** mode.



Match on Parent HCO records

Administrators and data managers can now configure match rules that match on the parent HCO records of the HCP record; for example, the parent HCOs of John Smith can be compared during loading. This gives users more flexibility for matching records.

This enhancement applies to **HCP** and **HCO Features** on the **Match Rules** tab. It is enabled by default for all countries.



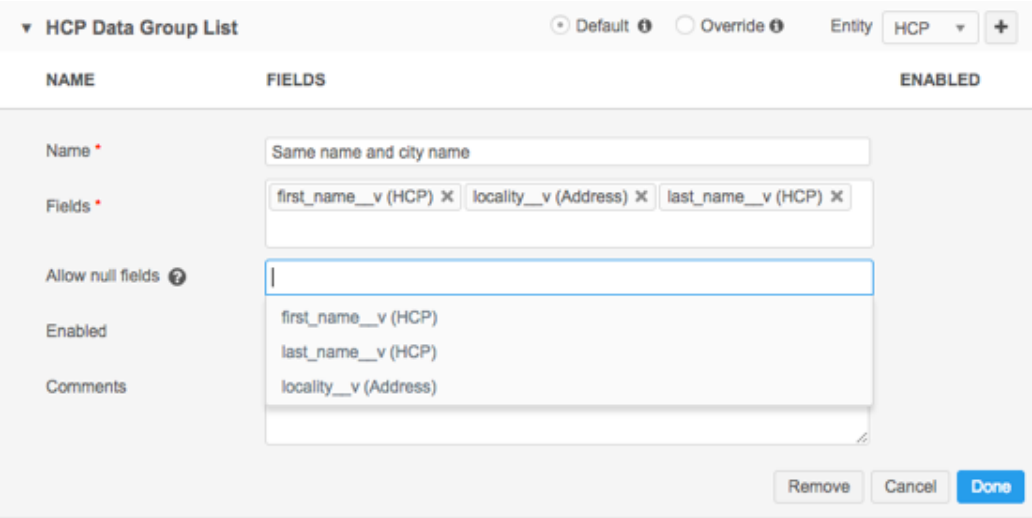
To use match on Parent HCO records in Basic mode:

1. Open your match configuration.
2. Click the **Match Rules** tab and scroll to the **HCP** or **HCO Features** section.
3. Using an existing feature, or a new feature, under the **Fields** list, select **Compare fields from Parent HCO records**. This enables you to match on parent HCO fields in the feature.
4. In the **Fields** list, select the HCO fields.
5. Complete the rest of the feature with the other options.
6. Click **Done**.
7. **Save** your changes.

Selecting null fields in data groups

Null matching enables users to indicate what Network should do about creating data groups if records do not have a value in a specific field. Previously, the null value options could be applied to the field level; for example, users could select `first_name__v` to be a null field, but not did have to select `last_name__v`. Both of these fields apply to the HCP entity.

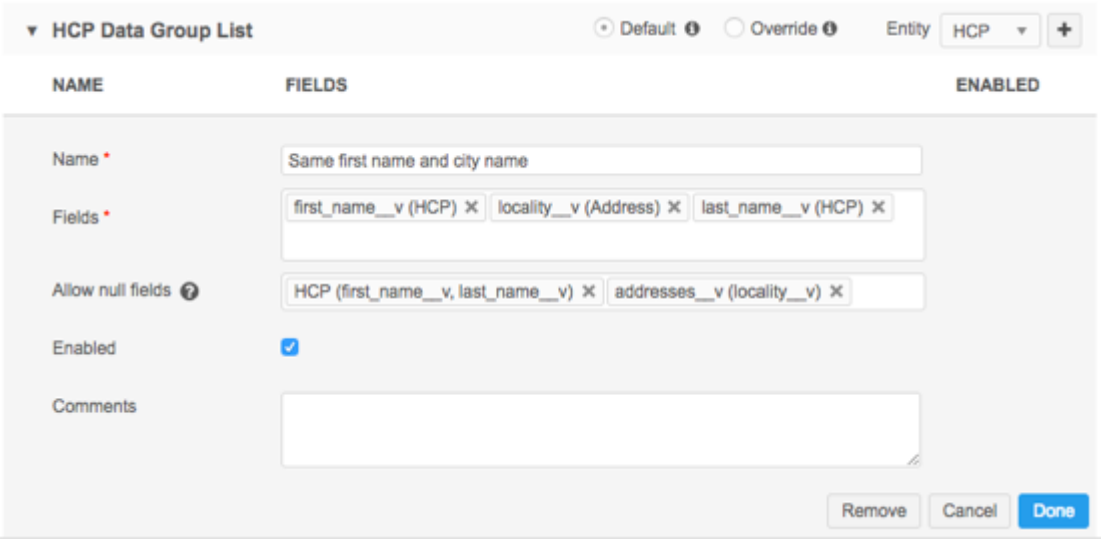
Previous behavior



Now, the null value options must be applied to all fields on an entity or child object. This helps data blocks to be created and processed more efficiently.

When users choose fields in a data group, those fields are available to select in the **Allow null fields list**. Fields will be grouped by entity or child object. For example, if `first_name__v` and `last_name__v` fields have been selected in the **Fields** list, they are grouped as the following in the **Allow null fields** list: `HCP (first_name__v, last_name__v)`. If another HCP field is selected in the **Fields** list, it is automatically added to the HCP group in the **Allow null fields** list.

New behavior



All new subscriptions will follow the new data block rules for null field values. Existing subscriptions will not be updated unless the values in the **Allow Null Fields** option are edited.

DATA GROUPS WITH NULL VALUES

Data groups are being created with null values, even if the **Allow null fields options** are false (no fields specified). This behavior is incorrect and is now fixed. Data groups will be created correctly according to the match configuration.

Home dashboard

The following topics include details on enhancements to the home dashboard in this release.

FEATURE ENABLED

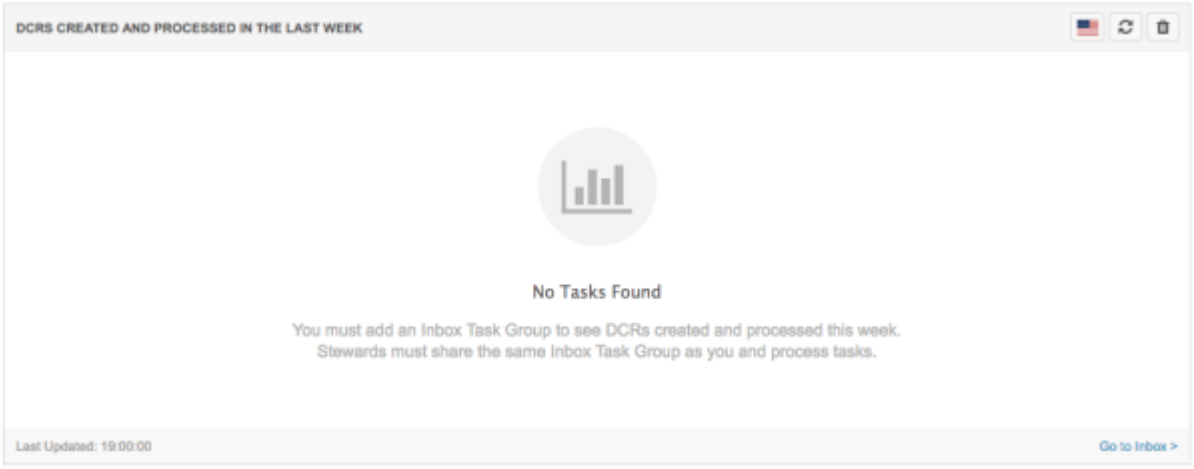
The Home Dashboard feature is enabled by default. Users no longer need to request the feature from Veeva Support. Administrators can enable or disable the feature for their Network instance from the **General Settings**.

It is available only to Data Manager and System Administrator users.

NO WIDGET DATA

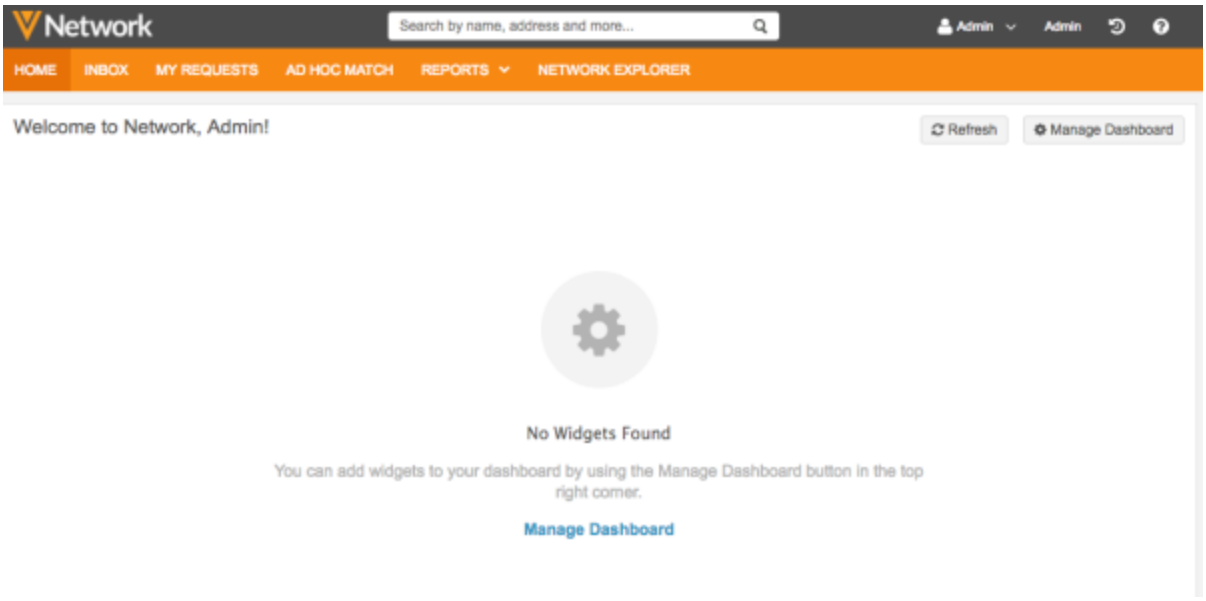
If data managers or administrators do not have data for a widget on their home dashboard, the widget provides details about how data can be made available.

For example, in the administrator's home dashboard, the **DCRs Created and Processed in the Last Week** widget provides tips about adding an Inbox Task Group and ensuring that data stewards share the same Inbox Task Group as that administrator user.



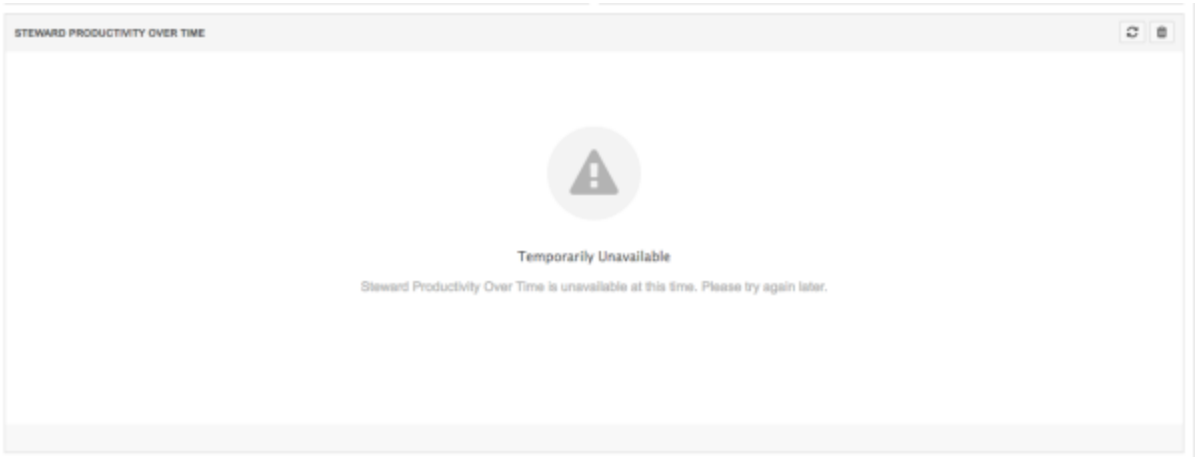
NO WIDGETS FOUND

If administrators or data managers have removed all of the widgets from their home dashboard, a message displays on the dashboard to advise them that they can use the **Manage Dashboard** button to add widgets again.



UNAVAILABLE WIDGETS

If widgets are temporarily unavailable, a temporarily unavailable message displays in the widget. For example, the **Data Quality Results** widget can be temporarily unavailable if the reporting server is down.

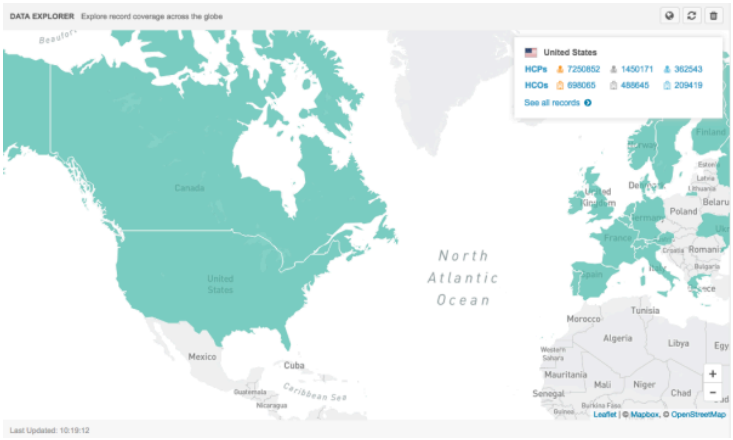


DATA EXPLORER UPDATES

The data explorer is updated with the following usability improvements:

- Countries with records are displayed with a higher contrast color for improved visibility.
- Data visibility profiles - the number of data visibility profiles that the user has determines the default view of the map.
    - One DVP - the map is zoomed into that country.
    - Multiple DVPs - the world map is the default view.
- Summary - clicking a country displays a summary count card.

- Country picker - Selecting a country has the following behavior:
    - Selecting a country zooms into that country and displays a legend in the top right corner.

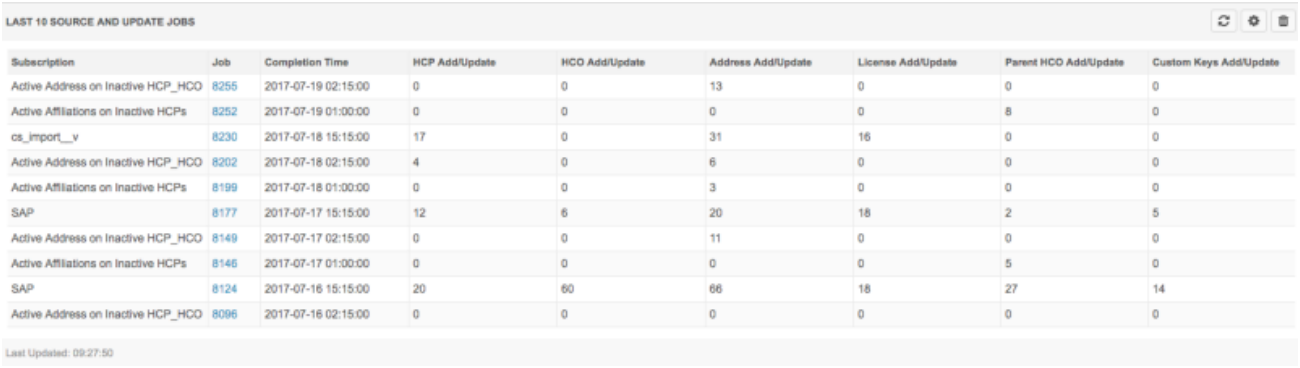


    - Zooming out or panning switches to the world view in the country picker.
    - Zooming in or clicking the same country keeps users in the country's context.

NEW WIDGET

The data manager home dashboard has a new widget called **Last 10 source and update jobs**.

The widget provides a summary on the most recent source subscriptions that have run. The table displays the entities and child objects that were added and updated during the job.



Subscription	Job	Completion Time	HCP Add/Update	HCO Add/Update	Address Add/Update	License Add/Update	Parent HCO Add/Update	Custom Keys Add/Update
Active Address on Inactive HCP_HCO	8255	2017-07-19 02:15:00	0	0	13	0	0	0
Active Affiliations on Inactive HCPs	8252	2017-07-19 01:00:00	0	0	0	0	8	0
cs_import__v	8230	2017-07-18 15:15:00	17	0	31	16	0	0
Active Address on Inactive HCP_HCO	8202	2017-07-18 02:15:00	4	0	6	0	0	0
Active Affiliations on Inactive HCPs	8199	2017-07-18 01:00:00	0	0	3	0	0	0
SAP	8177	2017-07-17 15:15:00	12	6	20	18	2	5
Active Address on Inactive HCP_HCO	8149	2017-07-17 02:15:00	0	0	11	0	0	0
Active Affiliations on Inactive HCPs	8146	2017-07-17 01:00:00	0	0	0	0	5	0
SAP	8124	2017-07-16 15:15:00	20	60	66	18	27	14
Active Address on Inactive HCP_HCO	8096	2017-07-16 02:15:00	0	0	0	0	0	0

Actions:

- Click the ID in the **Job** column to go to the **Job Details** page for more information about the subscription job.

REFRESHING THE HOME DASHBOARD

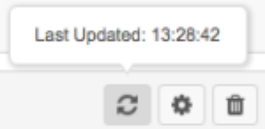
The query data in the widgets are cached for an hour. Users can click **Refresh** or navigate away and back to the dashboard to see new data after 60 minutes. Users can click **Refresh** at any time to see if there are changes in the data. If there are changes, the new results are displayed and the **Last Updated** time is

updated to the current time. If there are no changes in the data, the data doesn't refresh but the **Last Updated** time is updated to the current time.

If users log out of Network and log in again, the widget queries run again.

REFRESHING INDIVIDUAL WIDGETS

Refresh buttons are available on each widget so users can update individual widgets without updating the entire dashboard. Hovering over the button provides the **Last Updated** time of the widget.



The **Refresh** button on the Data Quality Reports widget does not re-run the data quality reports. You can run the reports again on the Data Quality Reports page.

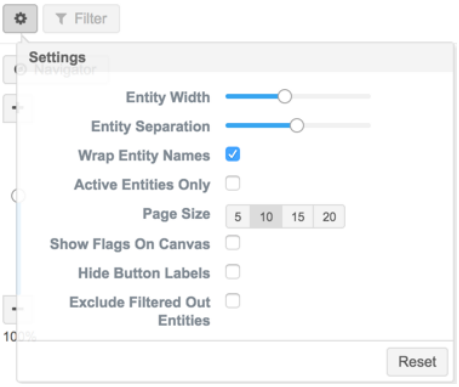
The **Refresh** button is dimmed for 30 seconds after the data is updated. This prevents refreshing the widget too often.

After 60 minutes have passed for a widget, the home dashboard is refreshed when users navigate away from the page and back again.

Network Explorer

WRAP ENTITY NAMES

This setting is enabled by default in all Network instances.



Users can now enable a setting so that the Network Explorer nodes display a larger portion of the entity name. Wrapping the entity name can help users to differentiate between entities. Previously, long entity names were truncated within one row, so it could be difficult to understand the hierarchy. For example, in situations where the parent HCO names are appended to a department name it was hard to understand the departments within the organization because all of the truncated entity names looked alike. Now users can see the longer names and understand the hierarchy at a glance.

Profiles

INACTIVE OBJECTS

On the Profile page, the font color for inactive values is darker. Users can read the text more easily and can still distinguish inactive object values from active object values.

Users

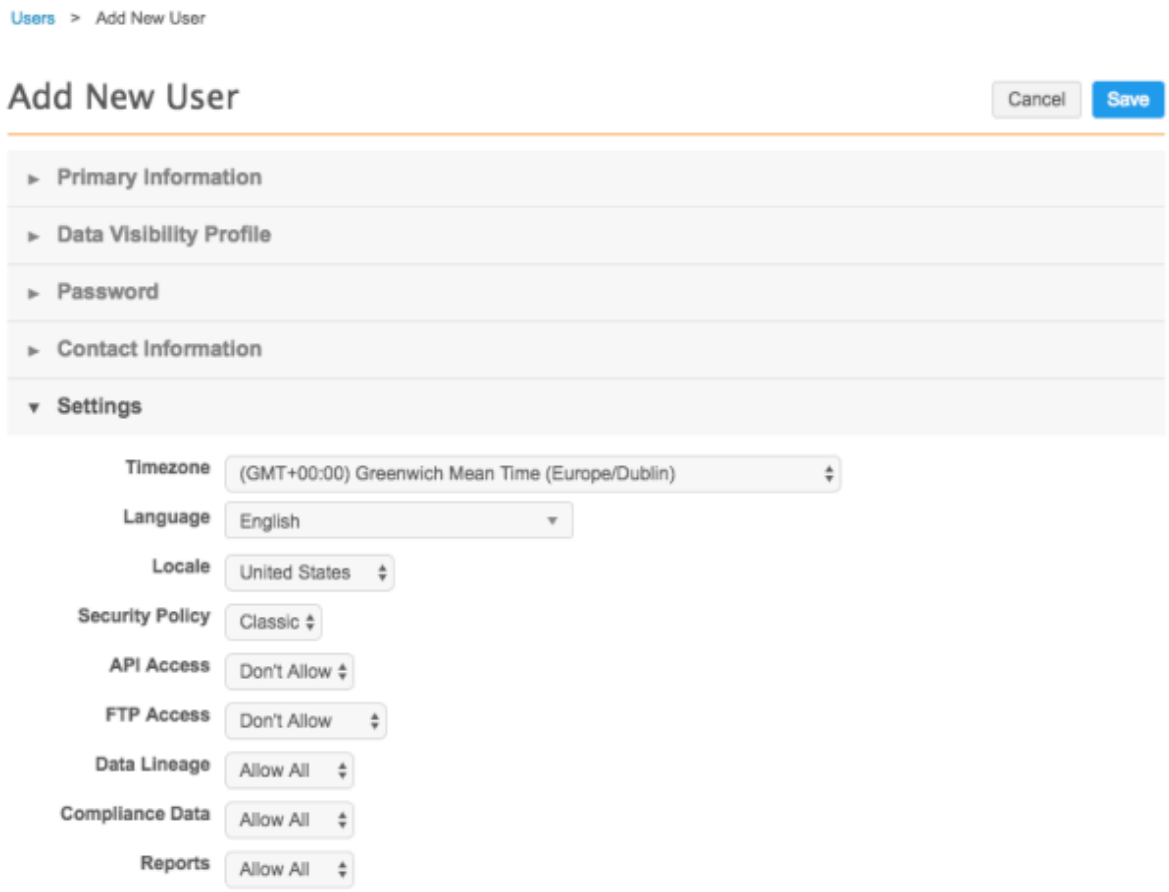
FEATURE ACCESS SETTINGS

New settings are available in the Add New User page so that administrators can simplify the Network user interface for users who do not need access to some features.

In the **Settings** section, administrators can remove access to these features in the user interface:

- **Compliance Data** - Controls access to the **Compliance Data** tab on the Profile page.
- **Data Lineage** - Controls access to the **Data Lineage** tab on the Profile page.
- **Reports** - Controls access, by user, to the **Reports** tab in the Network menu bar.

  Reports can be enabled or disabled globally using the General Settings. If Network Reporting is not enabled for your Network Instance, this option does not display on the Add New User page.



The default value for each setting is **Allow All**. To remove access to the feature in the UI, administrators can select **Don't Allow.**

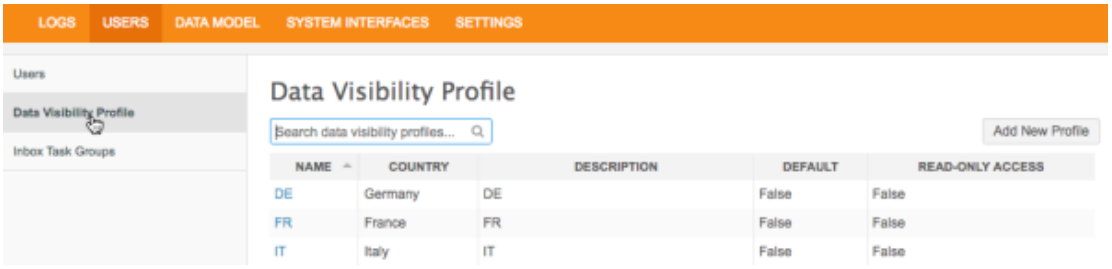
If **Don't Allow** is selected, the user cannot view or access the feature in the Network user interface.

Changes to access for users is visible in the **System Audit History** log.

Search

All of the Users features in the Admin console have been updated to include a search field so administrators can quickly find what they are looking for in each list. The search field has been added to the following pages:

- Users
- Inbox Task Groups
- Data Visibility Profile

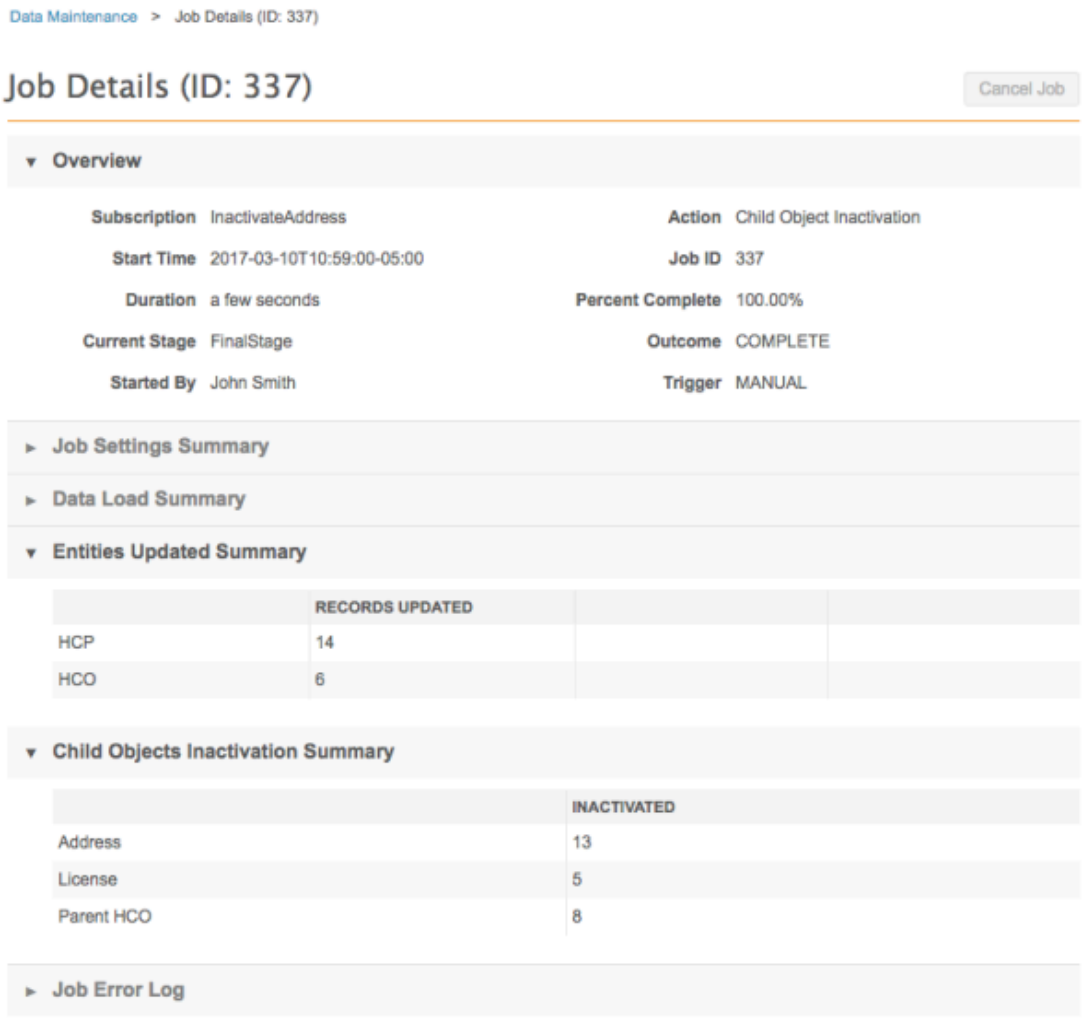


Data maintenance

CHILD OBJECT INACTIVATION

The Job Details page for child inactivation jobs is updated with the following changes:

- The **Processed Data Summary** section is renamed to **Entities Updated Summary**. This section displays the HCPs and HCOs that were updated during the job.
- The **Job Results Summary** is renamed to **Child Objects Inactivation Summary**.

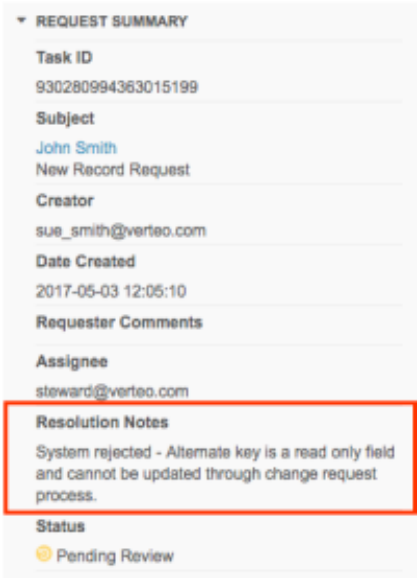


Data change requests

ALTERNATE KEYS

Alternate keys can no longer be included with add requests. The **Alternate Key** fields have been removed from the **Custom Fields** section. Alternate keys are generated by Network, so the option to submit values for alternate keys during an add request is not needed.

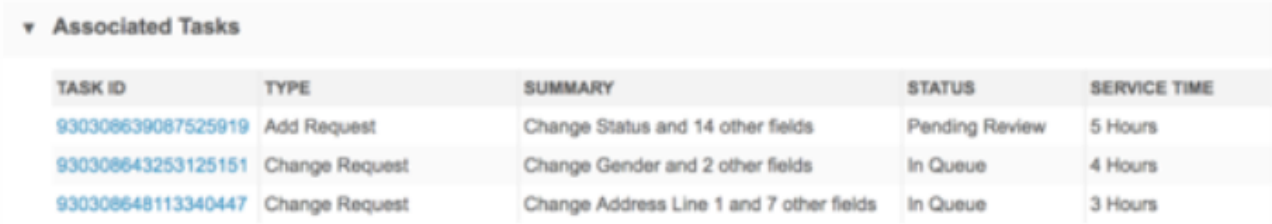
If alternate keys are submitted on add requests using the Network API, the field is auto-rejected. In the DCR, the **Resolution Notes** section in the **Request Summary** displays the automated message that the field was rejected because it included information in an alternate key field.



Associated Tasks

A new column, **Task ID**, is added to the **Associated Tasks** section on a profile. Data stewards can click the task ID link to be redirected from the Profile page to the DCR. Alternately, data stewards can right-click on the task ID link to open the DCR in a new tab.

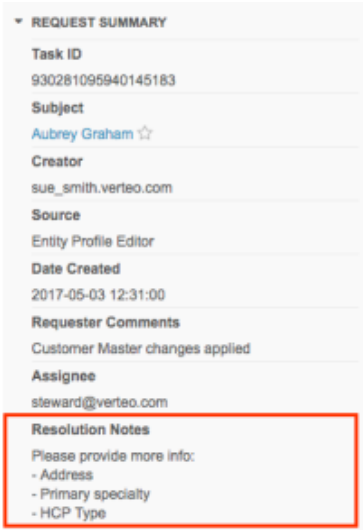
The **Associated Tasks** list is sorted by oldest task date.



This enhancement is also applied to the **Associated Tasks** table in DCRs.

Resolution Notes

When data stewards are processing DCRs, they can add line breaks in resolution notes so users can easily read the comments. These line breaks are supported by the Network-CRM bridge, so Veeva CRM users will see the properly formatted comments.



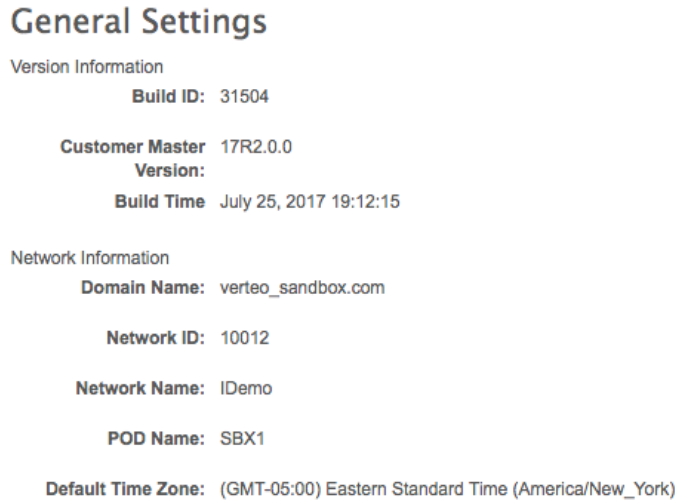
For API and DCR exports, the JSON response might contain "/n" whenever there are line breaks in resolution notes.

General updates

POD INFORMATION

Administrators can now see the POD information for their Network instance in the General Settings. When users are reviewing the trust site, trust.veeva.com, they can quickly know if an outage or planned downtime of a POD impacts them. Previously, POD information was available by contacting Veeva Support.

To view the POD name for your Network instance, in the Admin console, click **Settings > General Settings**.



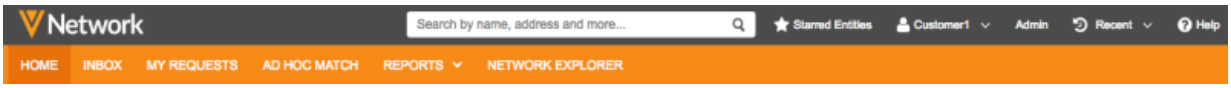
POD details

POD stands for “point of delivery”. In simple terms, it's the Network application server where your instance is hosted. PODs are located in data centers in the US and in Germany.

POD	Type	Location
VDM1	Production	Sterling, Pennsylvania, U.S.
VDM2	Production	Sterling, Pennsylvania, U.S.
VDM20	Production	Frankfurt, Germany
SBX1	Sandbox	Sterling, Pennsylvania, U.S.
SBX2	Sandbox	Sterling, Pennsylvania, U.S.
SBX20	Sandbox	Frankfurt, Germany

STARRED ENTITIES

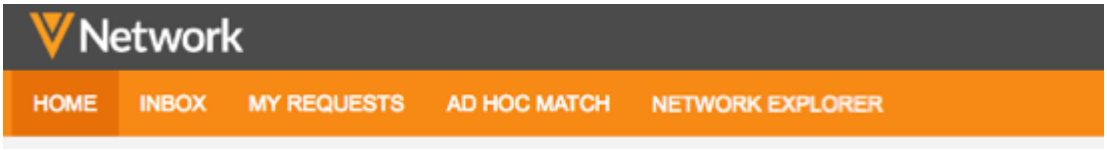
Users can now access their starred entities from the Network navigation bar. When the Home Dashboard feature is enabled, administrators and data managers can find their starred entities here. Standard users and data stewards can also access starred entities from their Home page.



Reports

REPORTS TAB

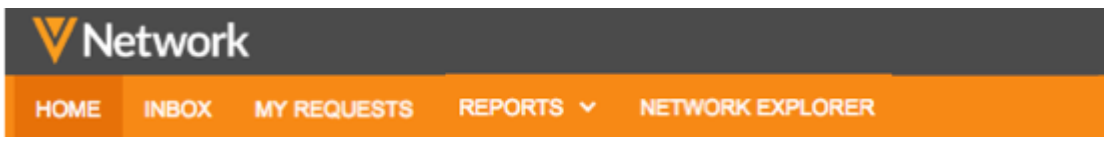
If the Reporting feature is not enabled in your Network instance, the **Reports** tab does not display in the Network menu bar.



Administrators can enable the **Reporting View** option in the **General Settings**.

Ad Hoc Match

If users do not have access to the Ad hoc match feature through their data visibility profile, the **Ad Hoc Match** tab does not display on the Network menu bar.



Concur Connector

The following topics describe updates for the Concur-Network integration.

FIELD MAPPINGS

The Concur mappings no longer include suggested descriptions. Previously, the fields would provide a name and a suggestion; for example, **Custom 14 (NPI Number)**.

If customers do not use the default mappings, the suggestions are not helpful. The field names will now include only the name; for example, **Custom 14**.

To find the Concur field name descriptions, you can use the Concur Configuration Report. To view the report in Concur, select **Administration > Expense > Configuration Report**.

Mapping the State address field

When you are mapping fields in the Concur Connector, be advised of the following:

- Map either the `State` address field or `Licensing Authority` field, but not both. Network will attempt to return the best address and state license for your search criteria, so mapping only the `State` field is recommended.
- It is recommended that the `State` address field is defined as a `List` field in Concur. If address state is defined as a `Text` field, then Network will not be able to return the best address in all cases.

CHILD OBJECTS IN SEARCH RESULTS

The Veeva Network data model permits multiple address, license, and relationships for a single Health Care Provider (HCP), however, the Concur data model only includes one address, license, or parent HCO. In this release, the Network-Concur Connector now returns the most relevant child object (address, license, parent HCO) based on the user's search criteria.

Example

A Concur user uses the following information to search for an HCP:

- Name: Bob Wood
- State: NY
- Institution: Memorial

Network has the following records that match the search query:

Network ID	Name	Specialty	Address 1	Address 2	Institution 1	Institution 2	License 1	License 2
3475245 5147687 6288	Bob Woods	Thoracic Surgeon	12 Bay St, Pawicky, NJ (active)	4 Elm Ave, New York, NY (active)	*Memorial Hospital (inactive)*	Atlantic Health System	NY 26NR058 41200	DEA F9123456 7
3475245 5261772 6976	Robert Wood	Thoracic Surgeon	47 Lincoln Way, Burlington, VT (active)	21 8th Ave, New York, NY (active)	University Health Network	Memorial Hospital	PA RN20687 0L	*NY 26NR082 35700 (inactive)*

Network considered the following criteria to return the most relevant results:

- Both records match on name
- Both records include an active address in the state of New York
- Robert Wood matches on the active parent affiliation. Bob Woods does not match because the parent affiliation is inactive.
- The best license is returned based on the following criteria:
    - Active licenses preferred
    - Matches the address state (NY)
    - Best state license flag = *true*
    - Last update time is more recent

Results

Based on the search considerations, the following results are returned to the Concur user:

Network ID	Name	Specialty	Address	Institution	License
347524552617726976	Robert Wood	Thoracic Surgeon	21 8th Ave, New York, NY (active)	Memorial Hospital	

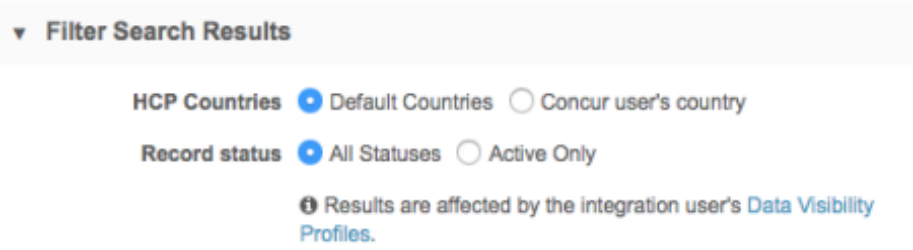
The child objects that best matched the search criteria were returned:

- Address - The active address in NY is returned because it best matches the search criteria.
- Parent HCO - The active parent HCO is returned.
- License - The active license that is from the same state as the address.

  Note that if you search for a DEA license number, it is returned in the search results instead of the state license.

FILTER SEARCH RESULTS

The Concur Connector now includes a new section where users can filter their search results.



Search results can be filtered for the following:

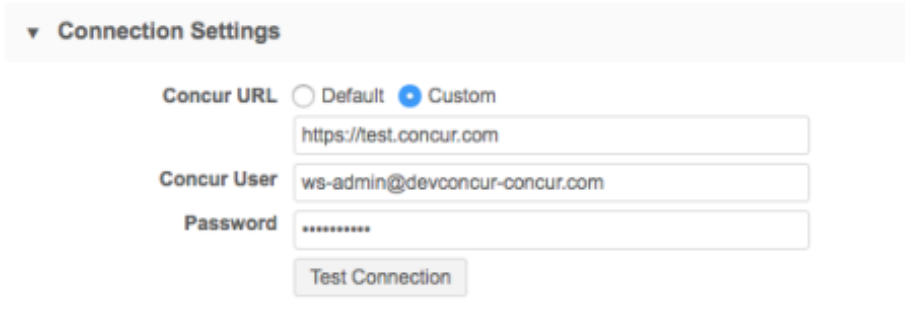
- **HCP Country**
  - Default Countries: Display results for all countries defined in the user's data visibility profile.
  - Concur user's country: Only display search results for the user's country.

  Previously, in the **System** section, Concur users could filter their search results on their country.

- **Record status**
  - All Statuses: Display results for all active and inactive records.
  - Active Only: Exclude inactive records from search results. This includes HCPs, HCOs, addresses, licenses, and parent HCOs. Excluding these records ensures a higher quality of search results and minimizes compliance risk.

CONNECTION SETTINGS

The Concur Connector **Connection Settings** section now includes the Concur URL. The default URL is for the production instance, but users can specify a custom URL.

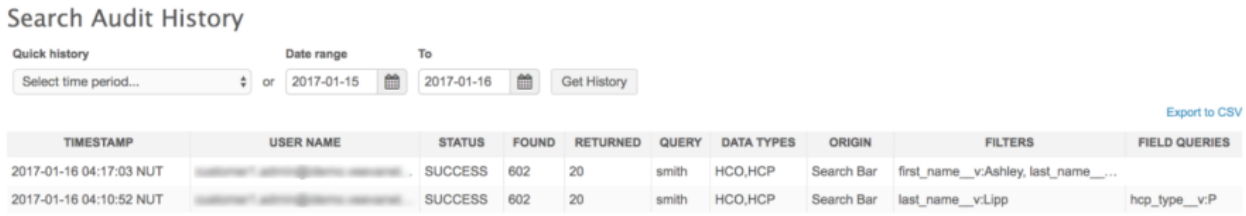


Note: When you are saving changes to your Concur Connector configuration, ensure that your browser does not unexpectedly autofill your credentials.

Logs

SEARCH AUDIT HISTORY

The search log now includes columns to show any **Filters** and **Field Queries** that were used in searches. Administrators can use the information in these fields to help with debugging. For example, administrators can use the value to reconstruct the search query to see what the user was searching for and to run those searches again.



To view the search log, in the Admin console, click **Logs > Search Audit History**.

API

The following updates have been introduced for the Network APIs in this release.

SEARCH API

The following updates have been introduced to v12 of the `Search` API for this release.

Parameters

The `Search` API is updated with following new parameters:

- `parenthcofilters` (optional) - The filters for parent HCO results. Parent HCOs in the `parent_hco__v` and `supplementalResults` sections will be returned if they pass these filters. The format is identical to filters but does not support filtering by child entities of the HCO.
- `nestChildObjectFieldQueries` - Use to define whether or not to apply nesting to child object clauses. This will convert a requested field query into a fuzzy matching filter on the same field. The default is false.

  Notes:

  - Filters do not return highlights when matching against these fields. It is assumed that all records matched the pattern for the specified field, so it is redundant to highlight this field.
  - Filters search the field directly, therefore if you are using this flag for a reference field you must supply the 'code' value not a reference label.
- `sortResultChildren` (optional)- For each search result that has Addresses, Licenses or Parent HCOs, those child objects will be sorted with the most relevant one being the first one. The default is false.

The `returnHighlights` flag must be set to *true* for the sort logic to work.

Address sort rules

- Highlights for Address fields.
- Field queries/filters for Address fields
- Primary address field (custom field type that is primary address) - Primary address is first (only one address can be primary).
- Record state (`record_state__v`) - Valid records first.
- Address status (`address_status__v`) - Active records first, then inactive records.
- Address type (`address_type__v`) - Professional (P), Professional and Preferred Mail (B), Mail Only (M), Address (U).
- Address ordinal (`address_ordinal__v`)

License sort rules

- Highlights for License fields.
- Field queries/filters for License fields.
- Record state (`record_state__v`) - Valid records first.
- License status (`address_status__v`) - Active records first, then Inactive records.
- License type (`license_type__v`) - State licenses first.
- Best state license (`license_status__v`) - Best state license first.
- `sortResultChildren` - For each search result that has Addresses, Licenses or Parent HCOs, those child objects will be sorted with the most relevant one being the first one. The default is false.

  The `returnHighlights` flag must be set to *true* for the sort logic to work.

Parent HCO sort rules

- Highlights for Parent HCO fields.
- Field queries/filters for Parent HCO fields.
- Primary Parent HCO field (custom field type that is primary affiliation) - Primary affiliation is first (only one Parent HCO can be primary).
- Record state (`record_state__v`) - Valid records first.
- Parent HCO status (`parenthco_status__v`) - Active records first, then inactive records.
- Is Primary relationship (`is_primary_relationship__v`) - Primary relationship first.

The `filters` parameter is updated to include the following new enhancements:

- **Scope** - The ability to define filters that apply only to a specific entity type. Scope filters use the following aliases:
  - `hcp` - The person entity.
  - `hco` - The organizational entity.

Format

`&filters=<entity_type>.<field_name>:<value>`

Example

`&filters=hcp.specialty_1__c:ON`

This example applies filters to the HCP entity return search results only for HCPs who have a primary specialty in Medical Oncology (ON)

- **Collection fields** - The ability to search an `OR` condition across a collection of fields during search. The fields must be enabled in the data model to be included in the collection. Collection fields apply to the following aliases:
  - `credentials` - Applies to fields `credentials_1__v` to `credentials_5__v`.
  - `medical_degree` - Applies to fields `medical_degree_1__v` to `medical_degree_5__v`.
  - `specialty` - Applies to fields `specialty_1__v` to `specialty_10__v`.

  Format

  `&filters=<entity_type>.<collection_field_name>:<value>`

  Example

  `&filters=hcp.specialty:ON`

  This query will check all HCP's specialties (`specialty_1__v` to `specialty_10__v`) that equal ON. If any of the specialties equals ON, the HCP is returned in the search results.