Veeva Network MDM

Veeva Network MDM 26R2.1.1 Release Notes

October 2026

Contents

About these Release Notes 6

Release dates 6

Subscribe to release notifications 6

Software releases and maintenance 6

Release Notes and Data Governance documents 6

Browser requirements 6

Release Note updates 7

What's new 7

Key dates for 26R2.1 7

Features 7

Data Governance 9

Network Widgets 10

Hide addresses on account profiles 10

Supported widgets 10

Hide addresses 10

Profiles 11

Display hidden relationships in the Revision History 11

What are hidden relationships? 11

Show hidden relationships 12

Impact to other Network MDM features 12

Search 13

Customize search results display 13

Highlights 13

Supported objects 14

Supported fields 14
Supported search displays 14
Impact to existing search results 14
Default search layout 14
Process for adding a search result layout 16
Configure a search result layout 17
Assign the search result layout to a DVP 18
Assign users to the DVP 19
Clone layouts 19
Logs 19
Inbox 20
Suspect match tasks 20
IQVIA OneKey Connector 21
IQVIA OneKey system support for country groups 21
Supported systems 21
Create a country group 23
Existing IQVIA OneKey systems 23
Validate countries during data load 24
Supported systems 24
Job warnings 24
Record access in the Search and Retrieve APIs 25
Supported APIs 25
Supported systems 25
Required permissions to access records 25

OpenData subscriptions **27**

Download unmerged OpenData records 27

Automatically download unmerged records 27

Users **29**

Restrict Admin permissions 29

Supported users 29

Impact to existing users 29

Supported features and functions 30

Admin Permission Set 31

Logs 32

Admin settings **33**

Use NEX rules for workflow settings 33

Supported workflow settings 33

NEX Rule enhancements for workflow settings 34

Define NEX rules 34

Exporting configurations 35

New configuration packages 35

Existing configuration packages 35

Security **36**

Single sign-on mappings 36

Supported user types 36

Mappings file 37

Validating the mapping file 37

Creating the user 37

Updates to Transport Security Layer ciphers 38

Impact to existing customers 38

About these Release Notes

These Release Notes describe all features that will be included in Veeva Network MDM 26R2.1.

RELEASE DATES

- **Sandbox release** (version 26R2.1) - Friday, October 2
- **Production release** (version 26R2.1.1) - Friday, October 16

SUBSCRIBE TO RELEASE NOTIFICATIONS

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

Software releases and maintenance

- Veeva Trust Site

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

Release Notes and Data Governance documents

The documents are posted in the following locations:

- Veeva Connect - Join the Network MDM Community.

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

- Veeva Network MDM Online Help

For more release information, see About Network MDM Releases in the *Veeva Network MDM Online Help*.

Browser requirements

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

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

Veeva Network MDM is not supported on mobile devices.

Release Note updates

The following update has been added since the Early Release Notes document was published.

- **Network Widgets** - Administrators can now hide addresses on account profiles using the Always Display field setting in profile layouts.
- **Security** - To protect your data, a legacy Transport Layer Security (TLS) cipher is removed from publicly accessible Network FTP servers.

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

What's new

KEY DATES FOR 26R2.1

- **Early Release Notes available** - Friday, September 18, 2026
- **Sandbox release** - Friday, October 2, 2026
- **Production release** - Friday, October 16, 2026

FEATURES

The following key enhancements comprise the Veeva Network MDM 26R2.1 minor release.

		Enabled by Default?	ST	DS	DM	AD
Network Widgets - General						
Hide addresses on profiles	Administrators can now hide addresses on account profiles by clearing the Always Display field setting in profile layouts.	Config Req.	●	●	●	●
Profiles						
Revision History	Empty revisions are now identified as hidden relationships and display details.	Yes	●	●	●	●
Search						
Search results	Administrators can customize the fields that display in search results for different objects and countries	Config Req.	●	●	●	●
Inbox						
Suspect match tasks	Match highlighting for field values is now case-insensitive.	Yes		●	●	

		Enabled by Default?	ST	DS	DM	AD
IQVIA OneKey Connector						
Multi-country system configurations	Use country groups to define record management and field ownership rules for different countries within a single IQVIA OneKey system.	Config Req.			●	●
Validate country during data load	Records that are loaded for the IQVIA-OneKey system are now validated to ensure that the country is managed by IQVIA.	Config Req.			●	●
API access to OneKey records	OneKey records are returned in the Search and Retrieve API only if the country is included in the IQVIA OneKey system configuration.	Config Req.		Developers		
OpenData Subscriptions						
Download unmerged records	Newly created records from unmerges can be automatically downloaded during your OpenData subscription job.	Config Req.			●	●
User management						
Restrict access to admin functions	Use permission sets to remove access for adding and editing configurations in the Admin console.	Config Req.				●
Admin Settings						
Workflow settings	Administrators can now create flexible conditions for auto-approving DCRs and reviewing master rejections using Network expressions.	Config Req.				●
Exporting configurations	Single sign-on settings are no longer supported in configuration packages. SSO settings must be configured on each Network MDM instance.	Yes				●
Security						
Single sign-on	The mapping file to dynamically provision users can now assign Inbox Task Groups to Data Stewards so they have immediate access to their tasks.	Config Req.				●
TLS cipher	To protect your data, a legacy cipher is removed from publicly accessible Network FTP servers.	Yes				●

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

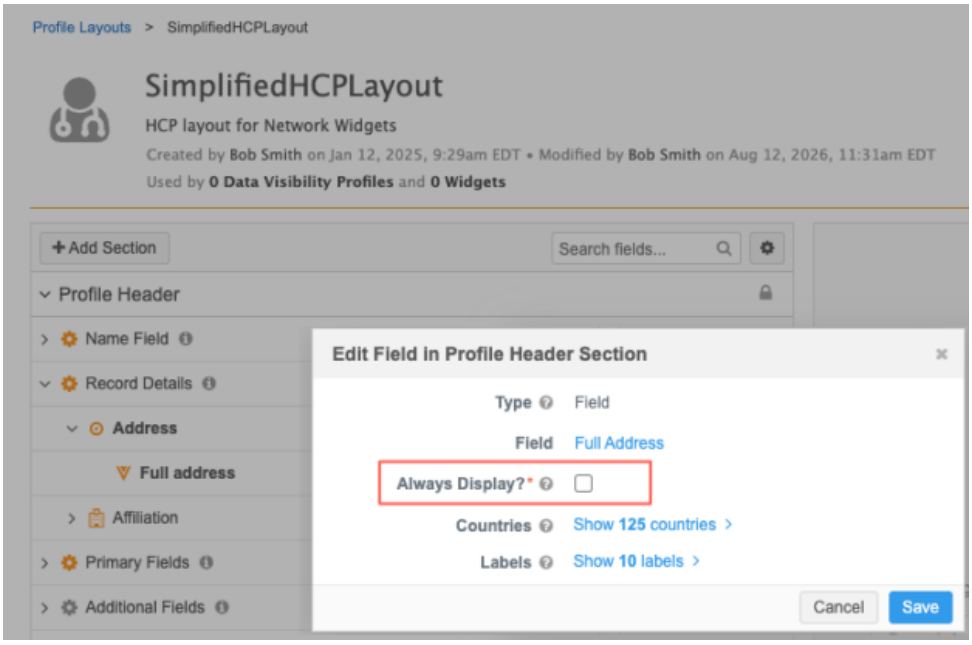
Data Governance

Fields and reference data updates are provided in the *Data Governance* document for every minor and major Network MDM release.

Network Widgets

HIDE ADDRESSES ON ACCOUNT PROFILES

Administrators can now hide addresses on account profiles using the field settings in the profile layout. The **Always Display** field setting now applies to Network widgets. When the setting is cleared, addresses are removed from profiles in widgets using that layout.



This enhancement is available by default. Administrators can configure the **Always Display** setting in profile layouts.

Supported widgets

- Profile widget
- Search widget

This change is applied to any Profile or Search widget using the profile layout.

Hide addresses

1. In the Admin console, click **Data Model > Profile Layouts**.
2. Open the layout assigned to your widget.
3. Under **Profile Header**, expand **Record Details**.
4. In the **Address** section, click the **Edit** icon next to the **Full Address** field.
5. In the **Edit Field in Profile Header Section** dialog, clear the **Always Display** setting.
6. **Save** your changes.

Addresses will now be removed from profiles in widgets that use the layout.

Profiles

Display hidden relationships in the Revision History

A record's revision history lists all changes to the record, but when an update involves a hidden relationship, no details display for that version. These empty updates are now flagged as hidden relationships and you can choose to view the details.

This enhancement is available by default. Users can enable the option to display hidden relationships on applicable records.

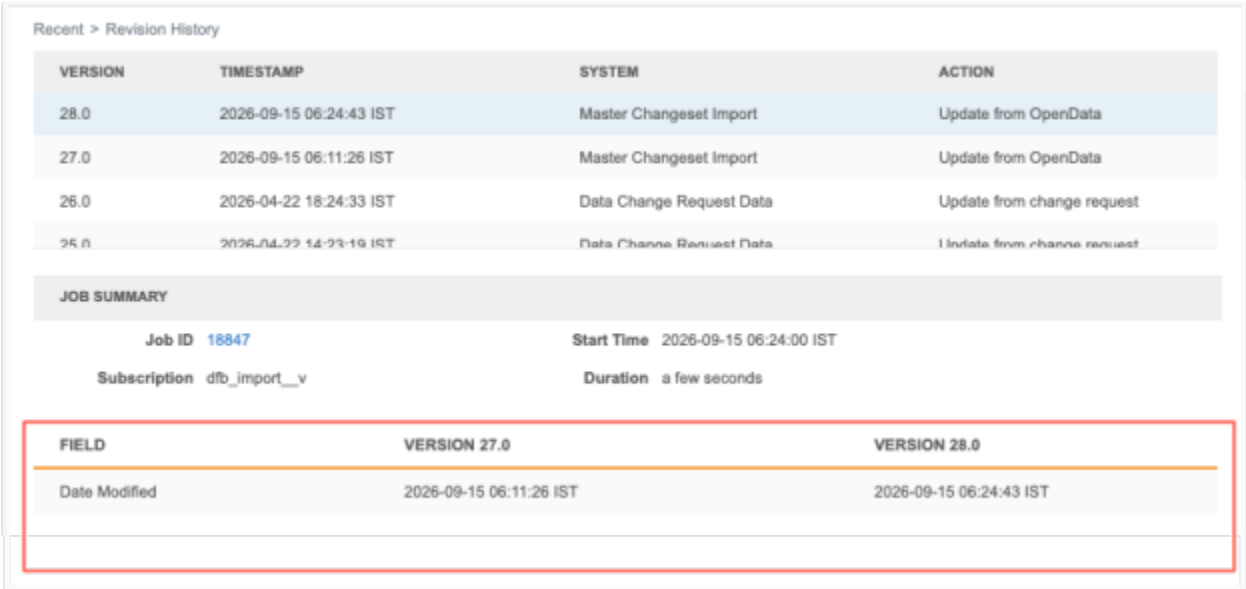
What are hidden relationships?

For completeness, each change creates a version in the record's revision history. This includes changes that OpenData makes to a record's relationships.

A hidden relationship occurs in the following situations:

- The parent HCO is not downloaded to your Network MDM instance.
- In 2-tier and 3-tier hierarchies for China, the relationship is dropped because it is not valid for the hierarchy structure.

When OpenData adds a relationship that is hidden to you for one of the reasons above, a new version is created, but only the modified date displays.

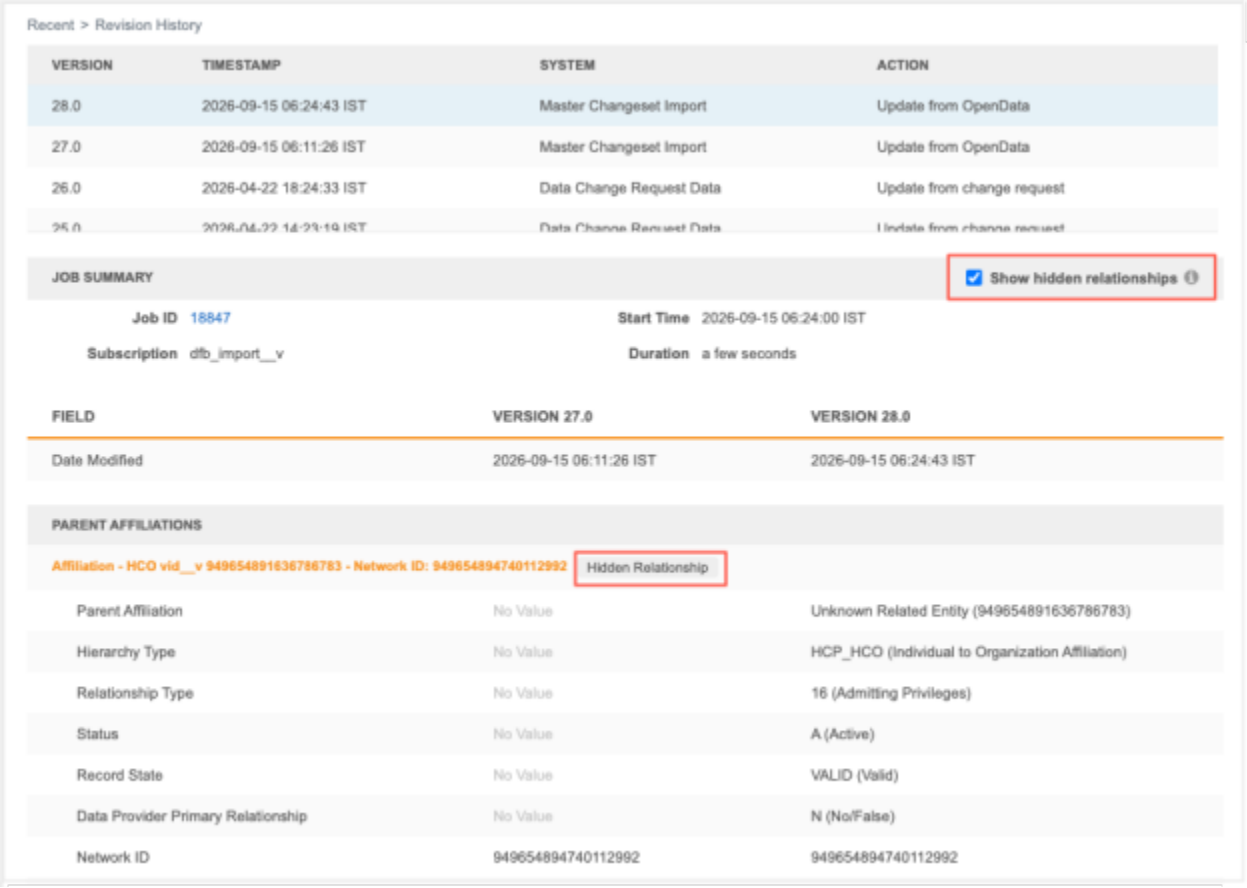


You can now view the details of the changes.

Show hidden relationships

When the revision involves a change to a hidden relationship, the **Job Summary** section now displays the **Show hidden relationships** option. The option is off by default.

Select the option to display the details made to the parent affiliation in the OpenData master instance.



When the **Show hidden relationship option** is on, hidden relationships are tagged so you can quickly identify those relationships.

Impact to other Network MDM features

Hidden relationships display only in the record's revision history.

They do not display in other features, including field revisions and revision history reporting.

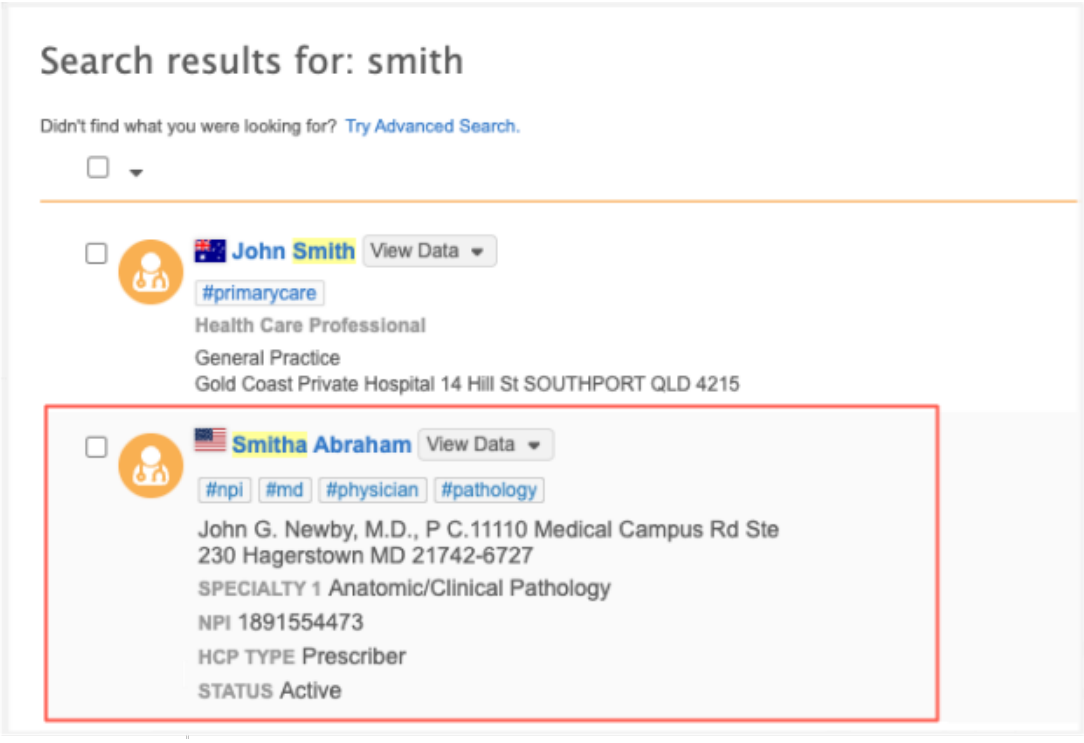
Search

CUSTOMIZE SEARCH RESULTS DISPLAY

Administrators can customize the fields to display in search results for different objects and countries. Replacing the default search result layout with country-specific details can help your users find and identify records faster.

Example

In this example, the search result for the US HCP uses a custom layout. The UK HCP result uses Network MDM's default search layout.



This feature is available by default in your Network instance. Administrators and Data Managers can define custom search result layouts.

Highlights

- Administrators can customize how search results display for each object.
- Search layouts are customized by country by assigning the layout to data visibility profiles (DVPs). Multiple countries can be defined for each layout.
- A maximum of 10 fields can be added to the layout.
- The display order of the fields can be customized.
- All users using the same DVPs will see the same layout for each object/country combination.

Supported objects

- Veeva standard objects (HCO, HCP)
- Custom objects

Supported fields

All fields related to the object can be added to the search result layout.

- Main object fields
- Sub-object and relationship object fields

Note: The field does not display in the search result if the field value is empty on the record.

Supported search displays

- Network Search - Quick search results
- Network Search - Search results page
- Parent HCO search on profiles and DCRs

Impact to existing search results

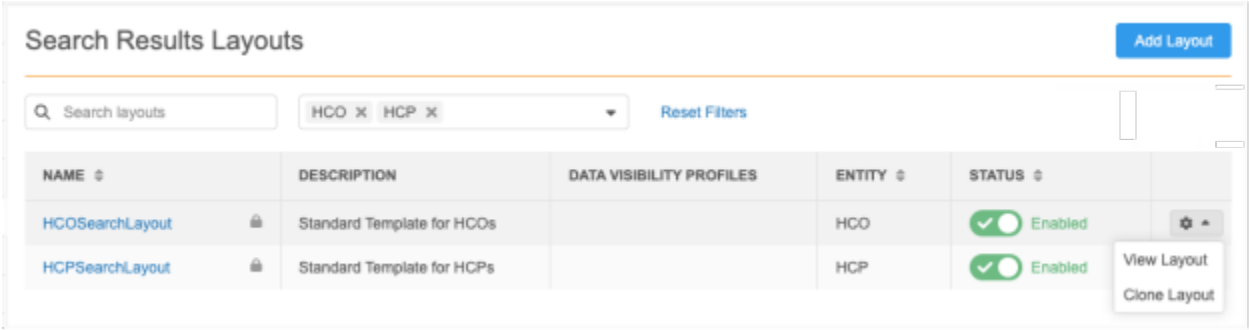
There is no impact to existing search results. The default layout displays until you customize it for an object.

Customizing the search result display does not impact the Network MDM search functionality; it changes only the way the results are displayed to users in the supported pages.

Default search layout

If no search display is configured, the default search layout displays.

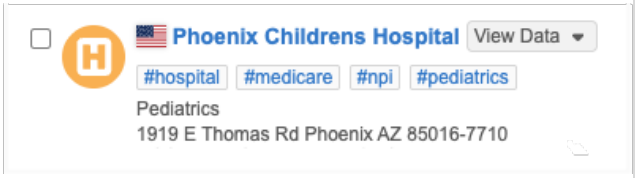
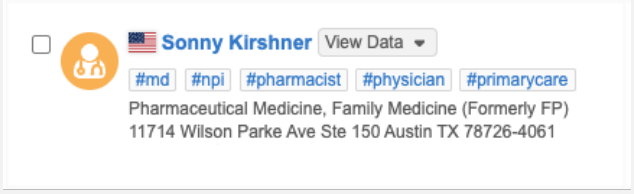
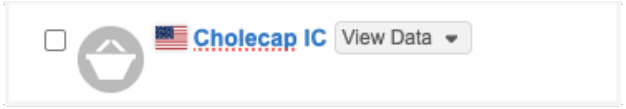
The Search Results Layouts feature contains the standard layout for HCOs and HCOs. These layouts are read-only, but they can be cloned to give you a starting point for your custom layout.



Default fields and display order for objects

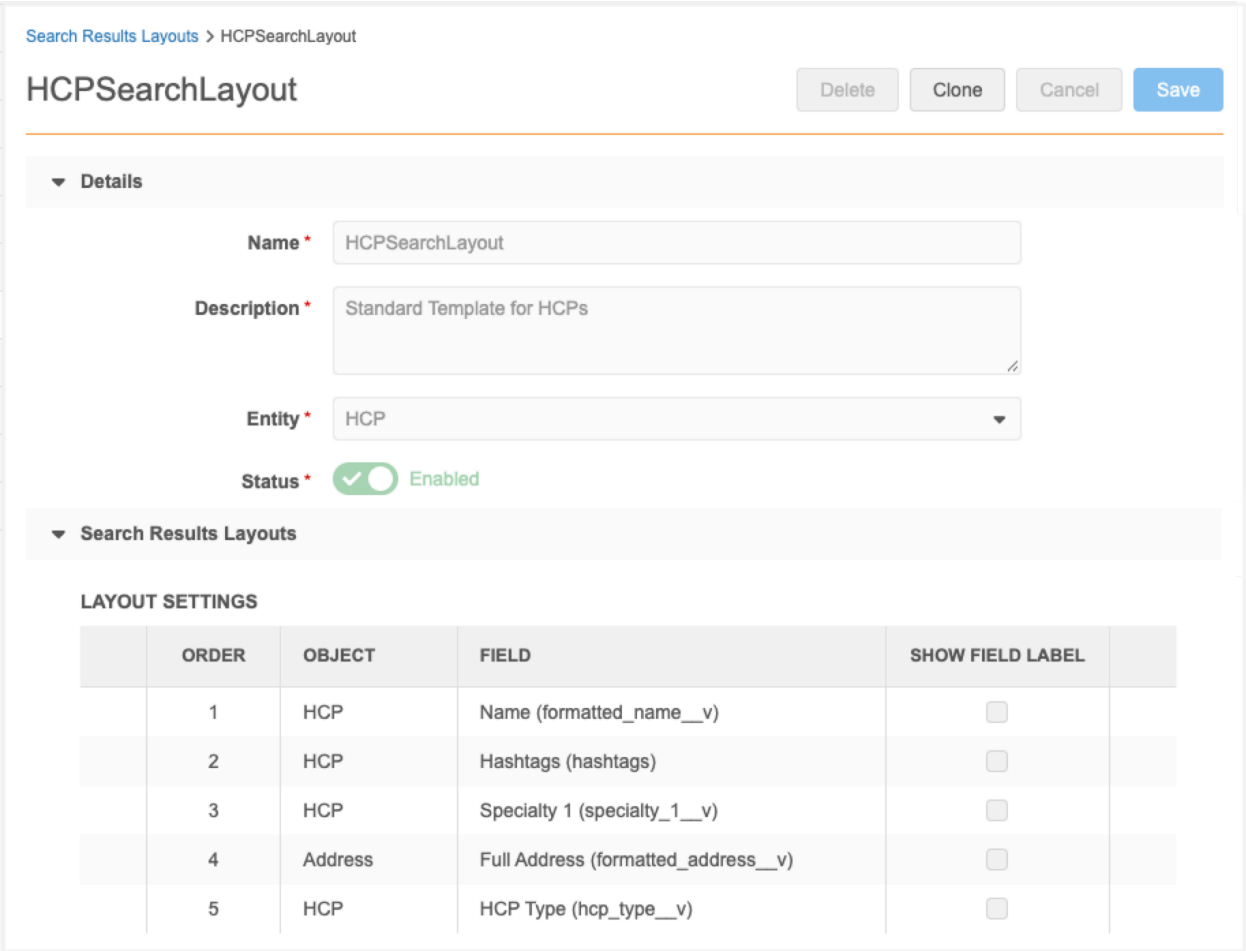
HCO, HCP, and custom objects have the following default display for search results.

Note: Country (flag icon) and object type (HCP/HCO/custom object icon) are always defined for each object.

Standard Template	Default Fields	Example
HCOs	1. Corporate Name 2. Hashtag 3. Specialty 1 4. Specialty 2 5. Full address (Rank 1/Network Calculated primary) 6. Key Networks	
HCPs	1. Formatted name 2. Hashtag 3. HCP type 4. Specialty 1 5. Specialty 2 6. Full address (Rank 1/Network Calculated primary)	
Custom Objects (no template)	1. Name	

The standard layouts apply to all countries.

Example – Standard template for HCPs



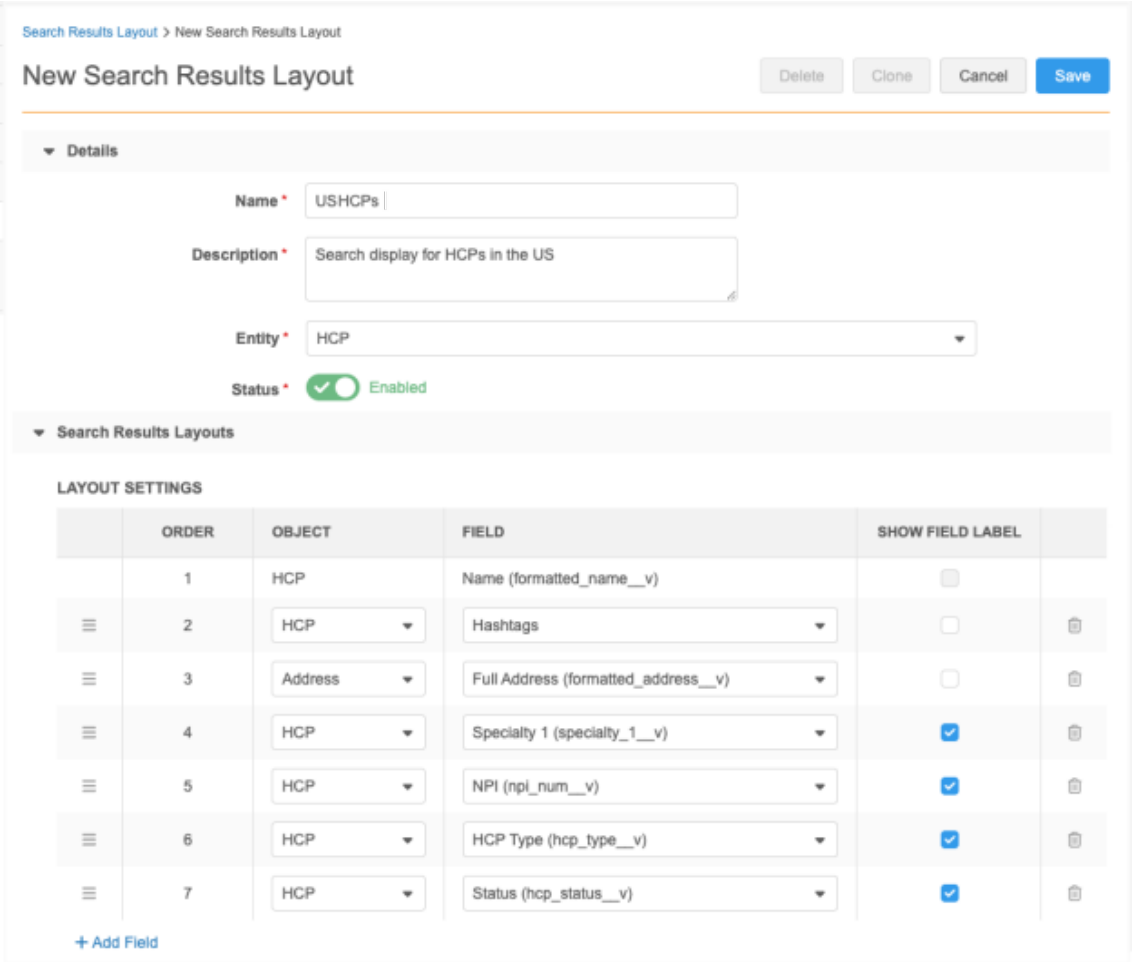
To customize the results by including different fields, defining the order in which the fields display, and applying it to objects for specific countries, create a custom search result layout.

Process for adding a search result layout

- Create a Search Result Layout for an object.
- Assign the layout to a data visibility profile (DVP) so it applies to specific countries.
- Assign users to the DVP.

Configure a search result layout

1. In the Admin console, click **Data Model > Search Results Layouts**.
2. Click **Add Layout**.
3. **Details** section - Define the following:
   - **Name** and **Description**
   - **Entity** - Choose the object that the layout applies to.
   - **Status** - The layout is enabled by default.
4. **Search Results Layout** - Choose the fields and the order that they should display.
   - **Object** - Choose the object that the field belongs to.
   - **Field** - Choose the field. The list is filtered for the defined object.
     Fields for all countries display.
   - **Show Field Label** - Select to add the field label to the search result. For example, HCP Type, Specialty.
   - **Reorder** - Use the **Handle** ☰ to move the fields into the desired position.
5. **Save** the layout.



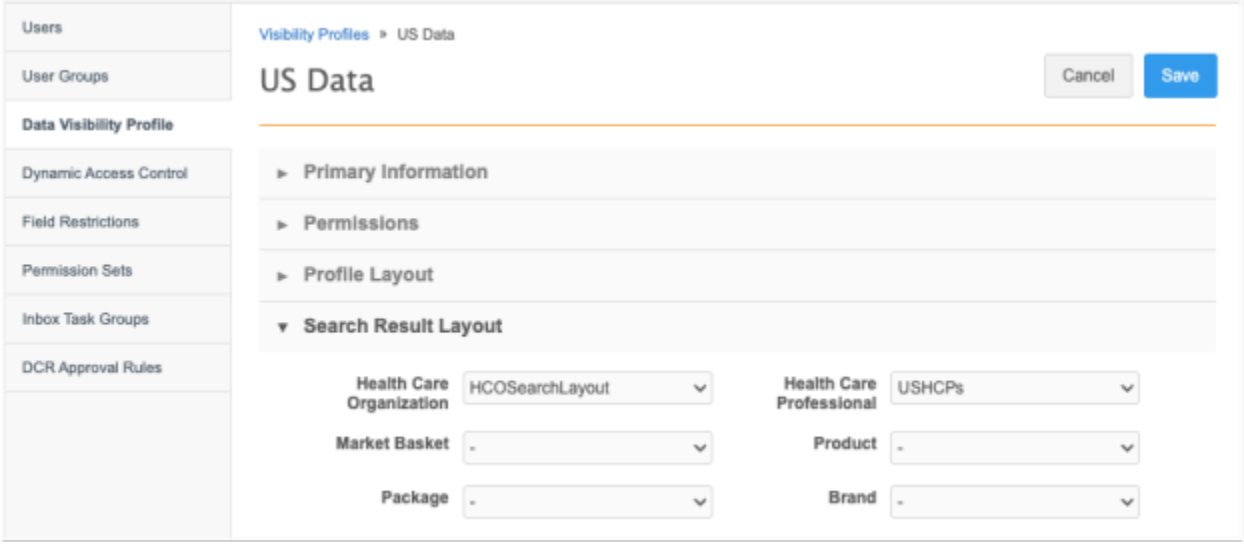
When the layout is ready, assign it to a data visibility profile. A search result layout can be assigned to multiple countries.

Assign the search result layout to a DVP

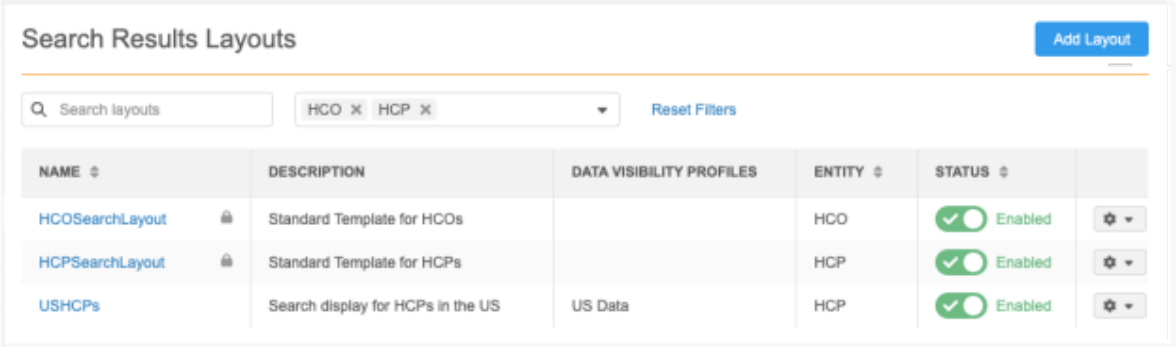
Data visibility profiles determine the records that users can access. Assign the layout to the data visibility profiles that should use the layout so users will see the customized display for that country.

Note: An object can have only one layout for each country.

1. In the Admin console, click **Users & Permissions > Data Visibility Profile**.
2. Open a DVP.
   A new section called **Search Result Layout** section is added to all DVPs. It includes all enabled objects in your Network MDM instance.
   For HCPs and HCOs, the default layouts are defined, `HCOSearchLayout`, `HCPSearchLayout`.
3. Expand the object and choose the custom layout.



4. **Save** your changes.
   The Search Results Layouts page is updated to identify the DVPs assigned to the custom layout.



Assign users to the DVP

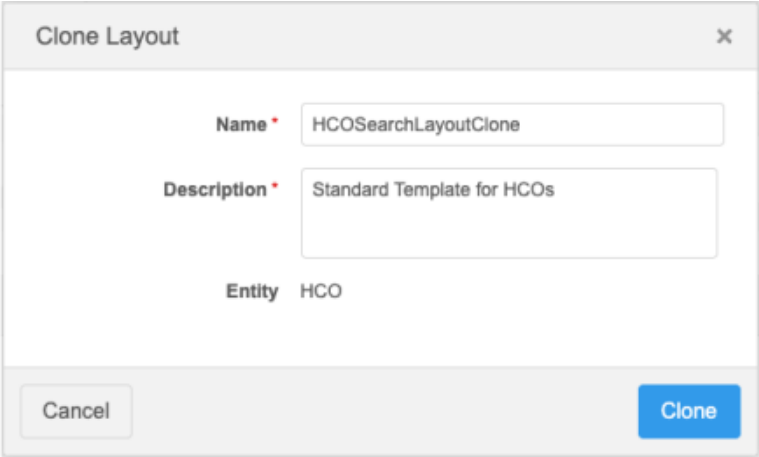
Each user account contains a **Data Visibility Profile** section. Assign the DVP to the user so they will see the search result layout display for that country.

Clone layouts

Any search layout can be cloned so you don't have to start over each time.

For example, if you want to create a layout similar to the Standard Template for HCOs, clone the layout.

1. On any layout configuration, click **Clone**.
2. In the **Clone Layout** pop-up, change the default **Name** and **Description** so it is meaningful for the new layout.



3. Click **Clone**.
4. In the **Layout Settings** section, make the changes to customize it.
5. **Save** your changes.

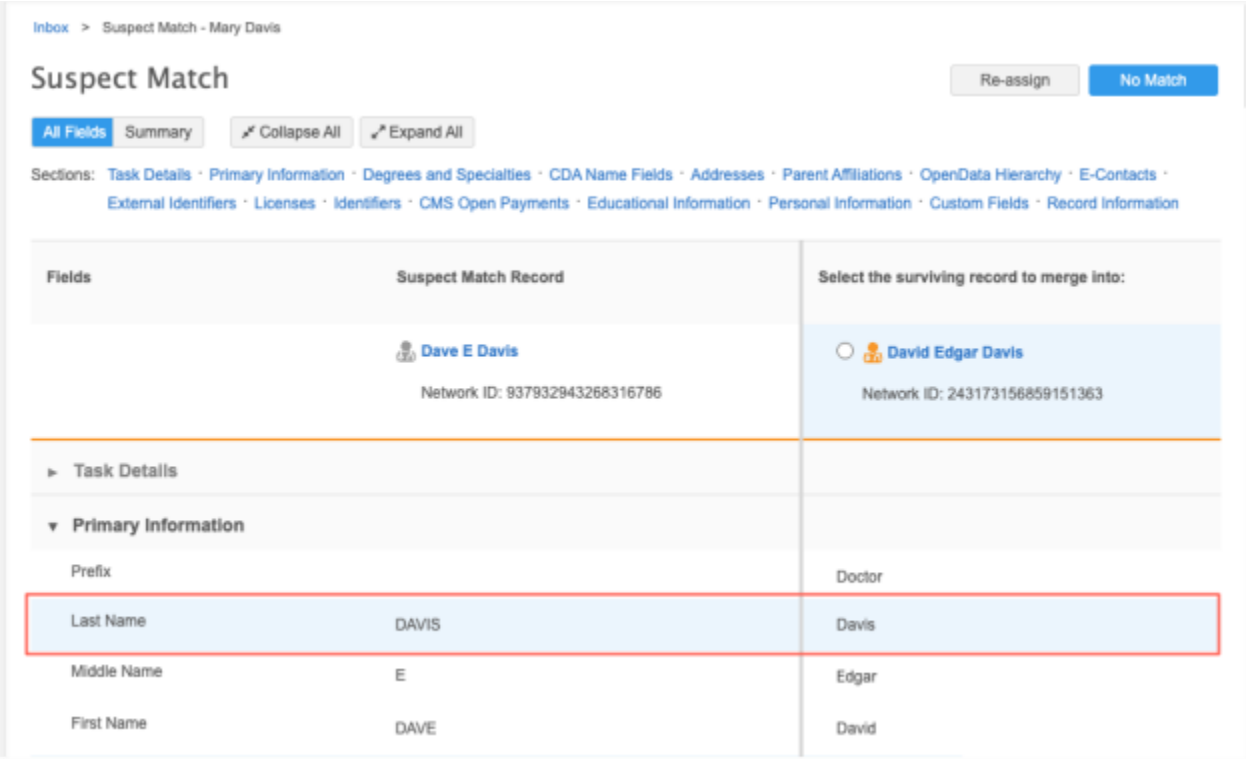
Logs

The System Audit Log tracks all new layouts and changes to existing layouts.

Inbox

SUSPECT MATCH TASKS

Matching field values containing different letter cases are now highlighted to help Data Stewards easily identify these matches. Previously, match highlighting was case-sensitive.



This enhancement is enabled by default.

IQVIA OneKey Connector

The Connector is a bi-directional connection with IQVIA® OneKey that seamlessly integrates OneKey as your third-party data provider for HCOs and HCPs within Network MDM.

The following enhancements have been added in this release. All enhancements are enabled by default.

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

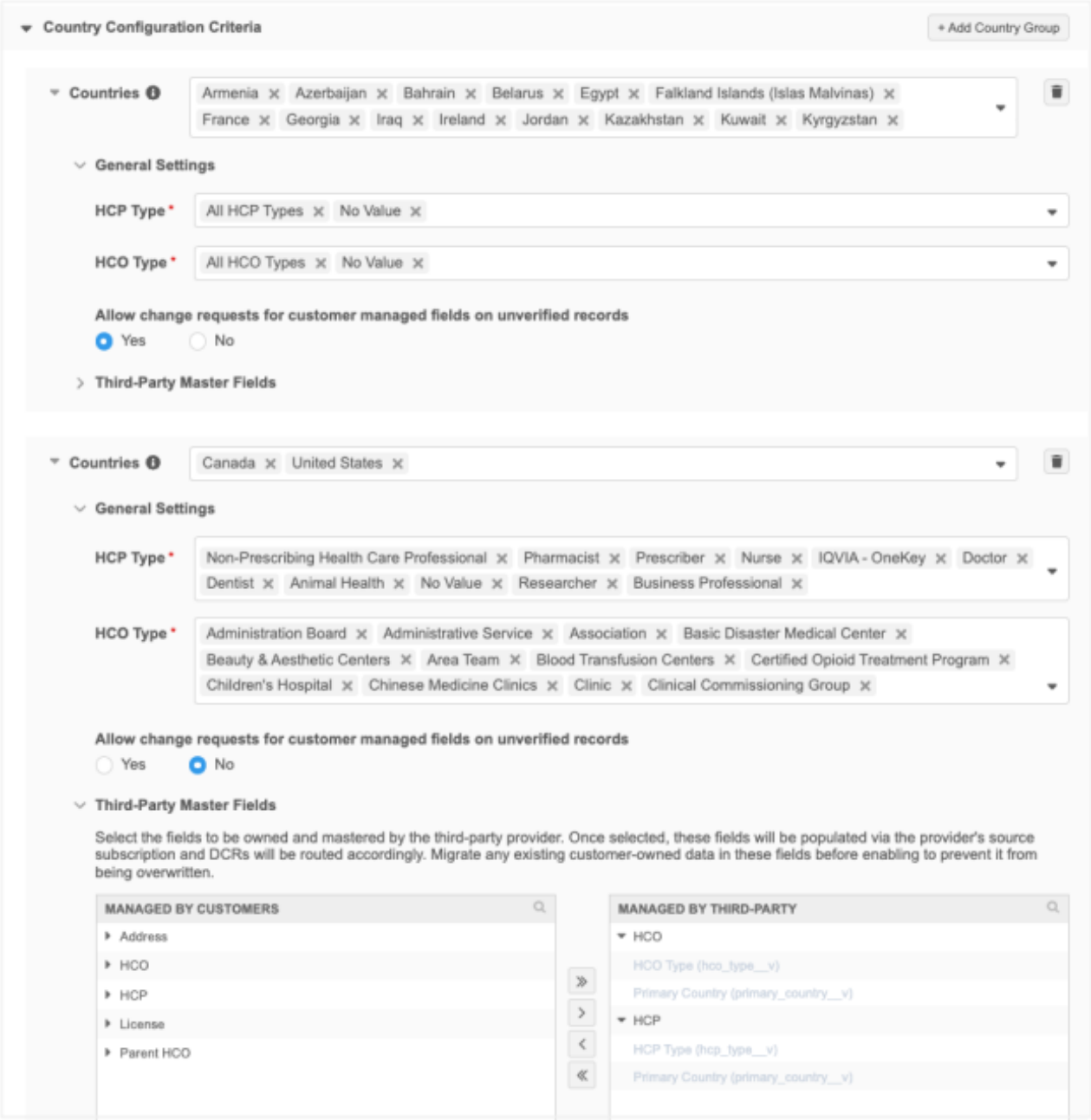
IQVIA OneKey system support for country groups

Third-party master systems, including your IQVIA OneKey system, now support multiple country-specific configurations. Using country groups, administrators can define record management and field ownership rules for different countries within a single system.

Supported systems

Country groups are supported for the following system types:

- IQVIA OneKey
- Custom systems defined as third-party master



Important: All countries mastered by IQVIA OneKey must be included in the system configuration. Data loading and API access now validates that the country is managed by IQVIA using this system. For details, see the Validate countries during data load and Record access in the Search and Retrieve APIs topics below.

Create a country group

Use a country group to define the records and fields that will be managed for specific countries.

1. In the IQVIA One-Key system, click **Add Country Group**.

   Define the following settings:

2. **Countries** - Select one or more countries to add to the group.

   A country can belong to only one group within the same third-party system. Countries that are managed by Veeva OpenData cannot be added.

3. **General Settings** - Choose the HCPs and HCOs by type that will be managed by IQVIA for these countries.

4. **Allow change requests for customer managed fields on unverified records** - Route DCRs for customer managed fields on unverified IQVIA records to be sent to local data stewards.

   This is helpful when users want to add information to a new record but the record is still pending approval from IQVIA.

5. **Third-Party master Fields** - Define the fields that will be managed by IQVIA for the countries in the group. Changes to fields in the **Managed by Third-Party** pane will be routed to IQVIA to process.

   To define the fields as IQVIA-managed, move the fields from the **Managed by Customer** pane to the **Managed by Third-Party** pane.

   Some fields are automatically moved to the **Managed by Third-Party** pane when the objects are defined as IQVIA-managed.

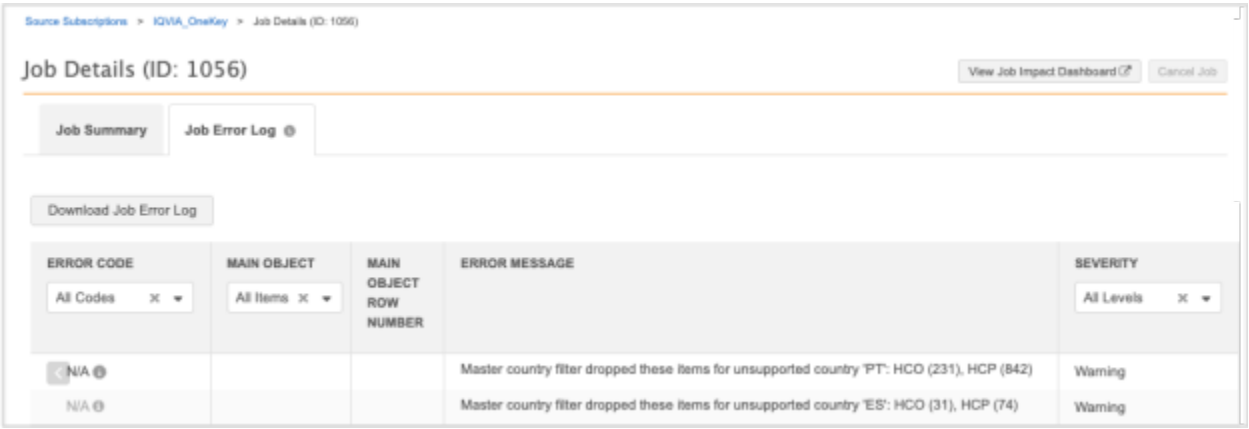
6. **Save** your changes or click **Add Country Group** to create another group.

Existing IQVIA OneKey systems

If you have a system configured, a country group is created for the existing countries, HCP, HCO, and field settings.

VALIDATE COUNTRIES DURING DATA LOAD

Records that are loaded for the IQVIA-OneKey system are now validated to ensure that the country is managed by IQVIA. If a country is not included in the IQVIA-OneKey system configuration, the record is not loaded. The Job Error Log displays a warning for each country with skipped records.



Supported systems

The country validation applies to IQVIA OneKey systems only.

Job warnings

When a record is loaded for the IQVIA OneKey system and the country is not managed by IQVIA, it could be for one of the following reasons:

- The country field (`country_cda__v`) is not defined for the record in the source file.
- The country is not included in the IQVIA OneKey system configuration.

If the country cannot be validated, the record is not loaded into your Network MDM instance.

The Job Error Log displays the following warning for each country with skipped records.

Error Code	Explanation	How to Resolve
N/A	Master country filter dropped these items for unsupported country <*'country_code'*> : HCO <*total_count*> , HCO <*total_count*>	Assign the country to a country group in the IQVIA OneKey system configuration or remove these records from the source file.

One warning occurs for each country.

The warning does not fail the job. The job can complete. Review the warning details and add the country to your IQVIA system configuration if required.

Record access in the Search and Retrieve APIs

Integration users searching for and retrieving records using the IQVIA OneKey system will only see the records from countries included in the IQVIA OneKey system configuration.

By automatically filtering API results to match your IQVIA OneKey system configuration, integration users receive cleaner, more focused responses containing only the exact country data they need. This built-in safeguard also protects data integrity by ensuring non-IQVIA records are never unintentionally exposed.

Supported APIs

OneKey records are filtered for the following APIs:

- Search
- Retrieve
  (Retrieve Entity, Retrieve Child Entity, Batch Retrieve Entities, Batch Retrieve Child Entities, Retrieve HCO, Retrieve HCP)

Supported systems

Filtering is supported for all third-party master systems, including your IQVIA-OneKey system.

For all other systems, records and fields are not filtered from the API response.

Important: If the Integration User has API access to all systems through their user profile, no record filtering is applied.

Required permissions to access records

To access IQVIA-managed records and fields for a country, the following configurations are required:

Integration User

The user profile must have the following settings defined:

- **Data visibility profile (DVP)** - Must be assigned to the DVP for that country
- **API access** - Must have access to the IQVIA-OneKey system

IQVIA OneKey system

- Must have the country defined in a country group

Example access scenarios

In this example, the Integration User needs to search for and retrieve IQVIA-managed records for France. The required configurations must be defined to access those records in the API.

Scenario	Integration User's User Profile		IQVIA OneKey System	Access to Country Records in the API?
	API access to IQVIA OneKey system?	Assigned to France DVP?	Country Group Contains France?	
1	Yes	Yes	Yes	Yes
2	Yes	Yes	No	No access
3	Yes	No	Yes or No	No access
4	No	Yes or No	Yes or No	No access

Result

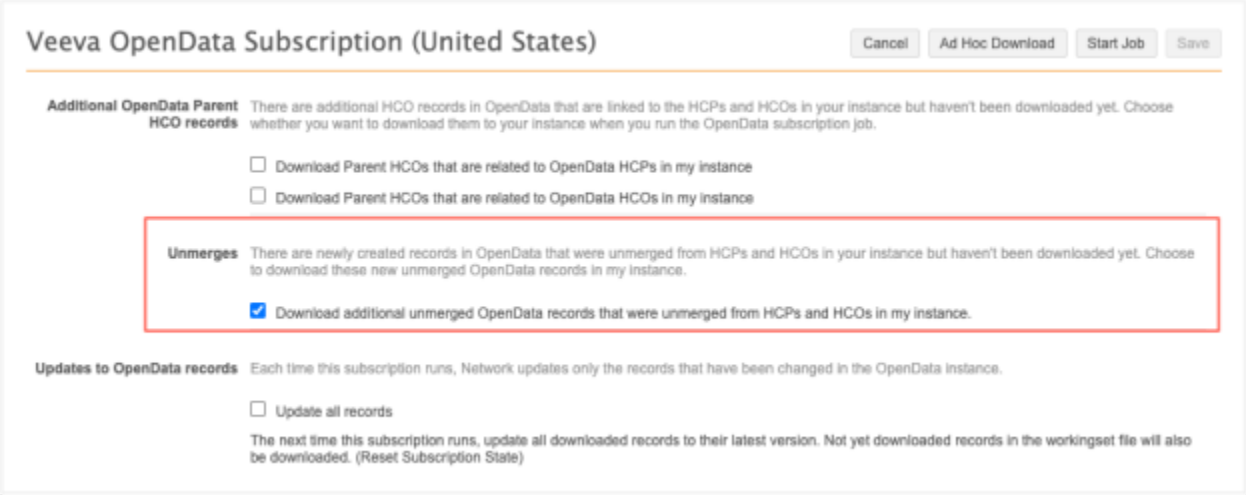
Only Scenario 1 provides access to the IQVIA-managed records for France.

If users search for a record they don't have access to, the API response contains only the Network ID for Search or an `Insufficient Access` error for Retrieve.

OpenData subscriptions

DOWNLOAD UNMERGED OPENDATA RECORDS

Administrators can now configure OpenData subscriptions to automatically download records that OpenData has unmerged. These are newly created records that were unmerged from HCPs and HCOs in your instance. Previously, unmerged records could be downloaded only using ad hoc download jobs.



This enhancement is available by default in your Network MDM instance. Administrators can choose to enable it in their OpenData country subscription.

Automatically download unmerged records

OpenData subscription configurations contain a new option to download unmerged records. The **Download additional unmerged OpenData records that were unmerged from HCPs and HCOs in my instance** option is not enabled by default.

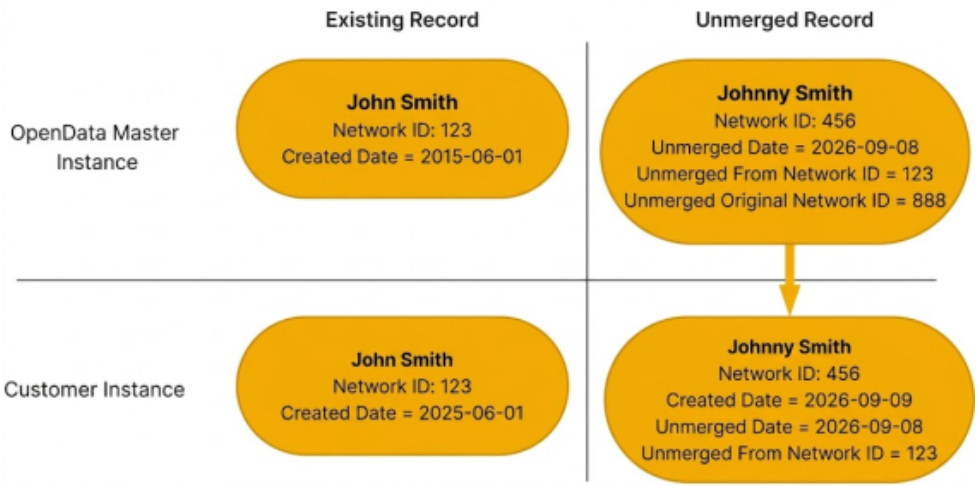
The newly created unmerged records are downloaded when the OpenData country subscription runs if the following conditions are met:

- The option to download unmerged records is enabled
- One of the original merged records is in your Network instance
- One of the original merged records is not unsubscribed in your instance.

Example

In this example, the OpenData record, John Smith, is downloaded in your Network MDM instance. OpenData unmerges the record. The Johnny Smith record is created.

If the option to download unmerged records is enabled, the Johnny Smith record will be downloaded the next time the OpenData subscription run. John Smith is already in your instance and it is not unsubscribed.

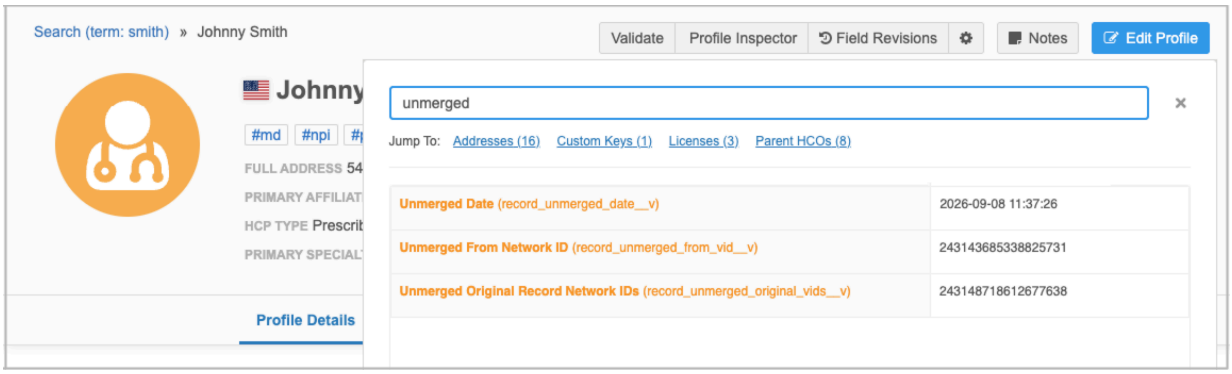


Unmerged fields

When an unmerged record is added to your instance, it contains the three fields that provide details about the unmerge.

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

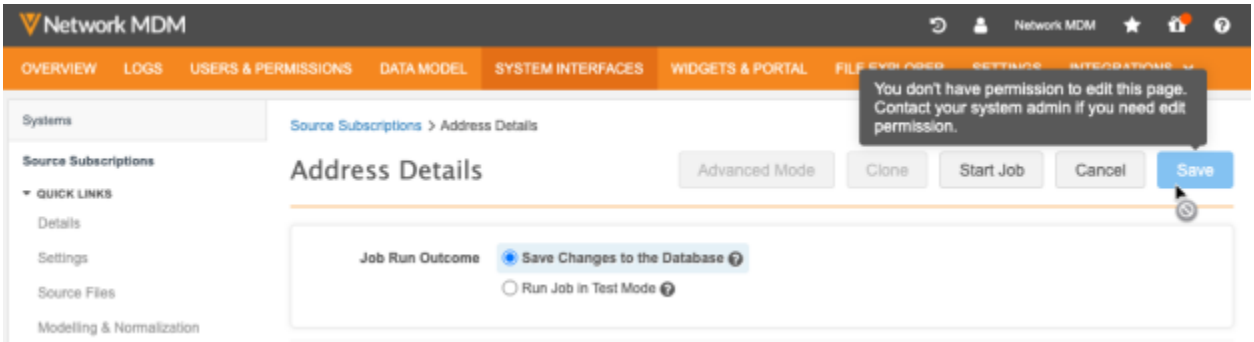
Tip: To quickly find the fields on the record, open the **Profile Inspector** and search for "unmerged".



Users

Restrict Admin permissions

Administrators can now use permission sets to control access to administrative functions. This can be especially useful for Data Manager users that have access to features in the Admin console but should not make configuration changes. Administrators can provide access to run subscriptions and view the configuration but restrict edit access to the features.



This enhancement is enabled by default.

Supported users

Admin permissions apply to user types that have access to the features in the Admin console:

- Data Manager
- System Administrator
- System and Data Admin

Impact to existing users

There is no impact to existing users. Data Managers, System Administrators, and System and Data Admins continue to have read and write access to the features.

Administrative users must explicitly use permission sets to provide or restrict access to admin features.

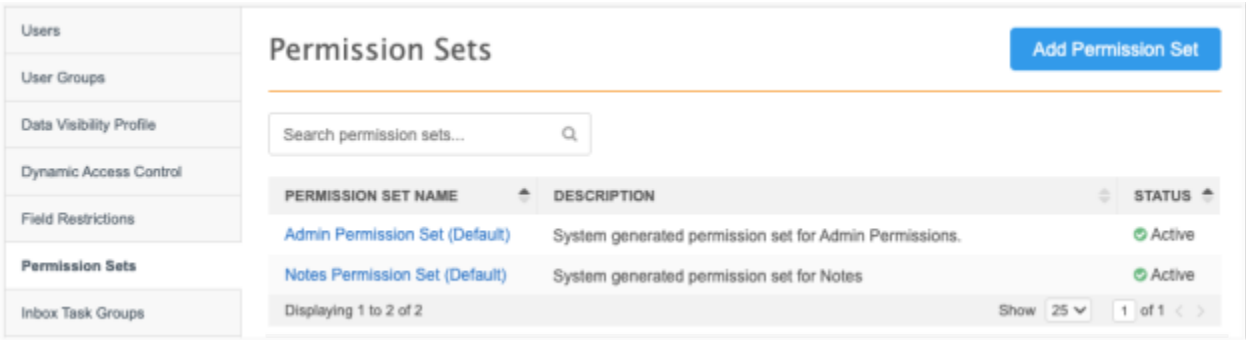
Supported features and functions

By default, users have add and edit access to these features. Restricting a feature reduces access to read-only mode and running subscriptions.

Feature	Add & Edit Functions	Read-Only (Add & Edit Disabled)
Data model		
Data domains	Add domain Add object Export Data Model Save objects Add fields Enable / disable fields Save fields	View
Reference Data	Add reference type Edit reference type summary Import reference codes.	View Export
System Interfaces		
Systems	Add system Save system	View
Source subscription	Add subscription Clone subscription Save subscription Access Advanced Mode	View Start Job
Target subscription	Add subscription Clone subscription Save subscription Export by Network ID	View Start Job
Veeva OpenData subscriptions	Create New Country Group Save subscription	View Start Job Ad Hoc Download
Match Configurations (Ad Hoc Match Configuration, Match Default Configuration, Add Request Match Configuration)	Save configuration	View
Match Rule Collections	Add Collection Save collection	View
Source Rankings	Save	View
Transformation Rules	New Rule Save rule Clone Delete	View

Admin Permission Set

A new permission set called `Admin Permission Set` is added to your Network MDM instance.

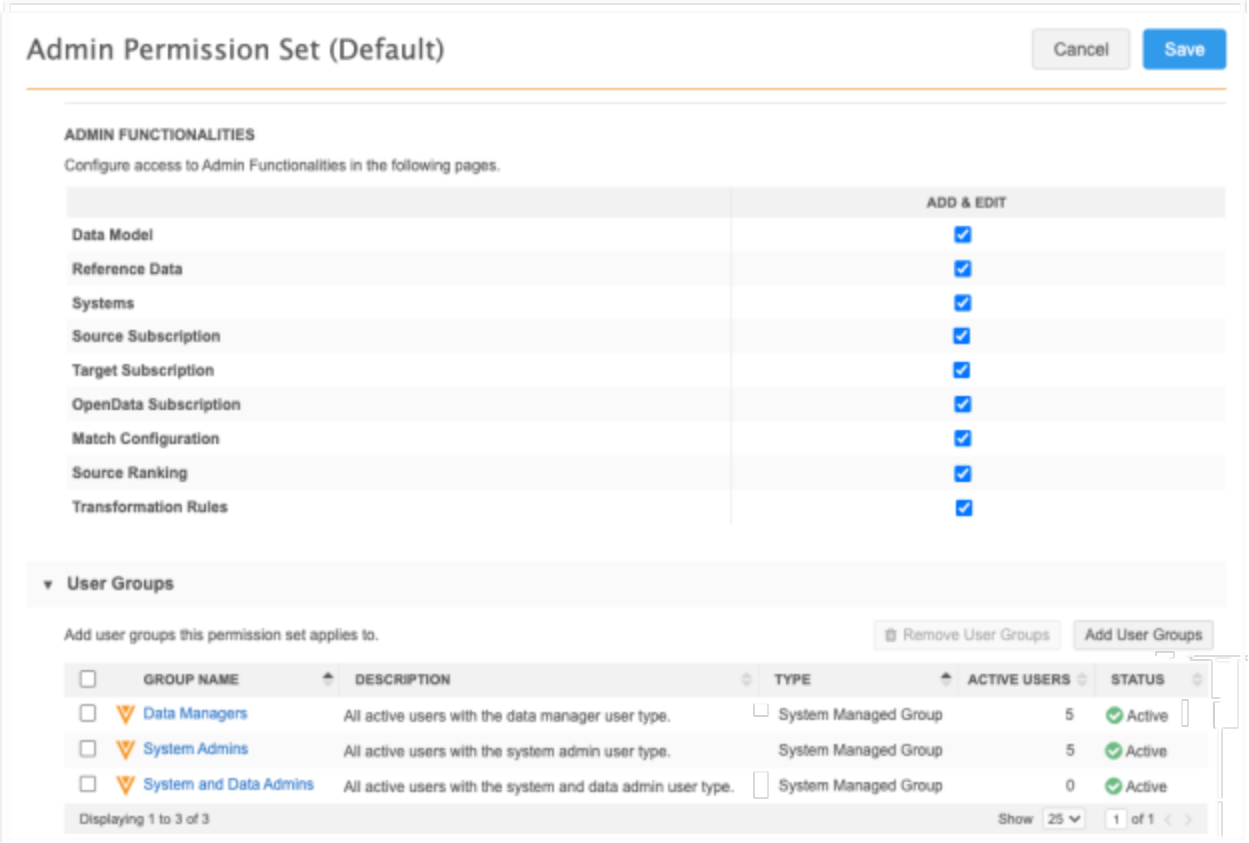


It includes the following system-managed user groups:

- Data Managers
- System Admins
- System and Data Admins

These groups contain all users of that type that are defined in your Network MDM instance.

All features in the **Admin Functionalities** section have **Add & Edit** permissions by default. This ensures that there is no impact to existing users.



Example scenarios

- To restrict these Admin features for Data Managers, remove the Data Managers user group from the Admin Permission Set.
- To restrict Admin features on a more granular level (for example, by user), create a new permission set and assign access by user.

If users are included in multiple permission sets, the highest permission level wins.

Logs

Changes to the permission sets are tracked in the System Audit Log.

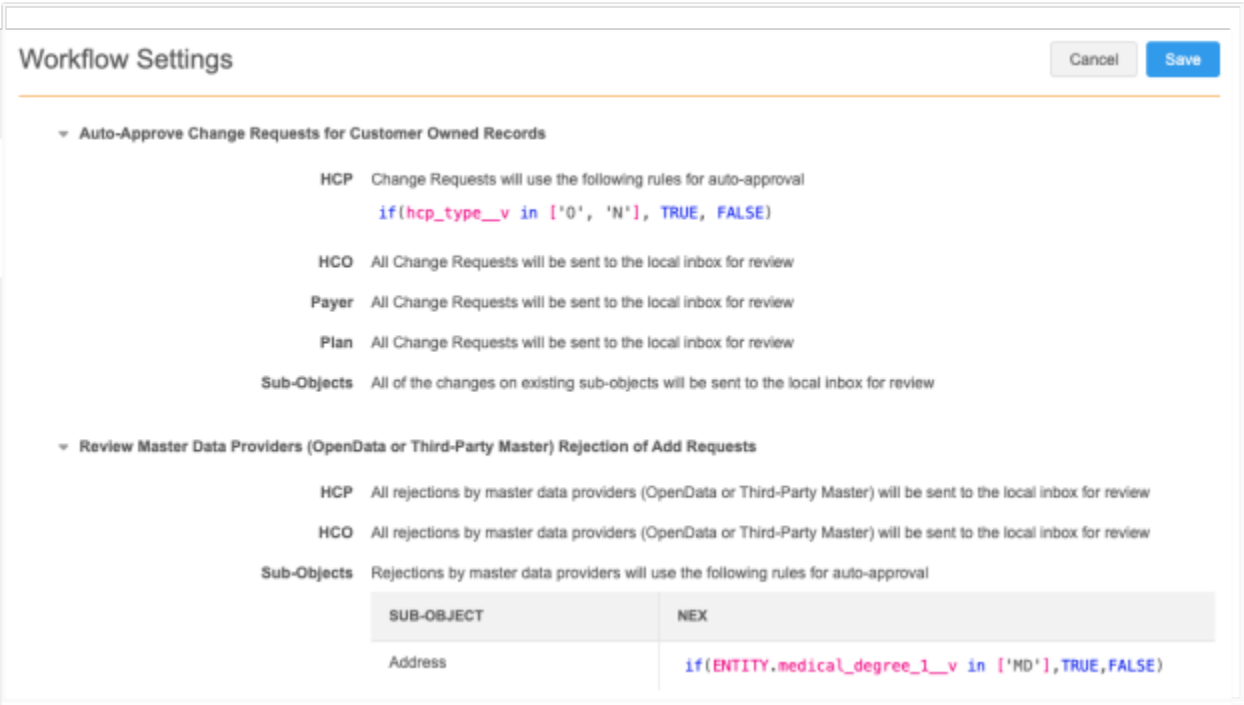
Admin settings

USE NEX RULES FOR WORKFLOW SETTINGS

Administrators now have more flexibility for configuring auto-approvals and review rejections in the workflow settings. Network Expression (NEX) Rules can be used to identify specific conditions.

Examples

- Review rejections on addresses based on the HCP or HCO value.
- Auto-approve specific sub-objects on HCPs, but not HCOs.
- Auto-approve add requests submitted by specific users.
- Auto-approve add requests for HCPs based on the HCP type.



This enhancement is enabled by default. Administrators can define NEX rules for the supported settings.

Supported workflow settings

- Auto-Approve Add Requests for New Customer Owned Records
- Auto-Approve Change Requests for New Customer Owned Records
- Review Master Data Providers (OpenData or Third-Party Master) Rejection of Add Requests

NEX Rule enhancements for workflow settings

To support the ability to define specific conditions for these settings, the following updates are made to Network expressions.

Workflow metadata

The following three fields can be used to in Network expressions:

- creator
- system
- source

Example: Auto-approve Add Requests for HCPs

```
if(DCR.creator == 'bob.smith@verteo.veevanetwork.com', TRUE, FALSE)
```

Use entity level fields in sub-object rules

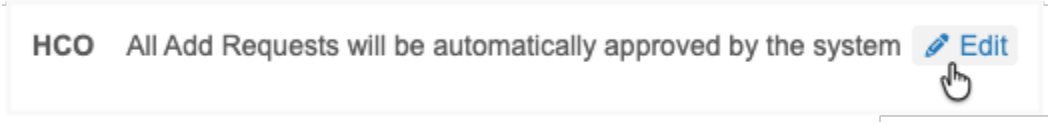
Create a condition for a sub-object based on a field value for the related entity.

Example - Review rejections for addresses if the HCP is an MD

```
ENTITY.medical_degree_1__v in ['MD']
```

Define NEX rules

1. In the Admin console, click **Settings > Workflow Settings**.
2. Hover over the setting that you want to change to display the **Edit** button.



3. Click **Edit** to display the available options for the setting. Select the option to use NEX.

4. Enter the Network Expression in the field.

   Tip: Comments can be added to explain the expression or add details for other users.

5. The NEX rule validates as you type the expression.
6. **Save** your changes.

The workflow setting is now to use the NEX rule for that object.

Exporting configurations

Single sign-on (SSO) configurations are no longer supported in configuration packages because they contain environment-specific details that cannot be transferred between instances. SSO settings must be configured within each instance.

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

New configuration packages

SSO settings cannot be added to export packages.

Existing configuration packages

If your package included SSO settings, the configuration package will fail when you try to import it to a target instance.

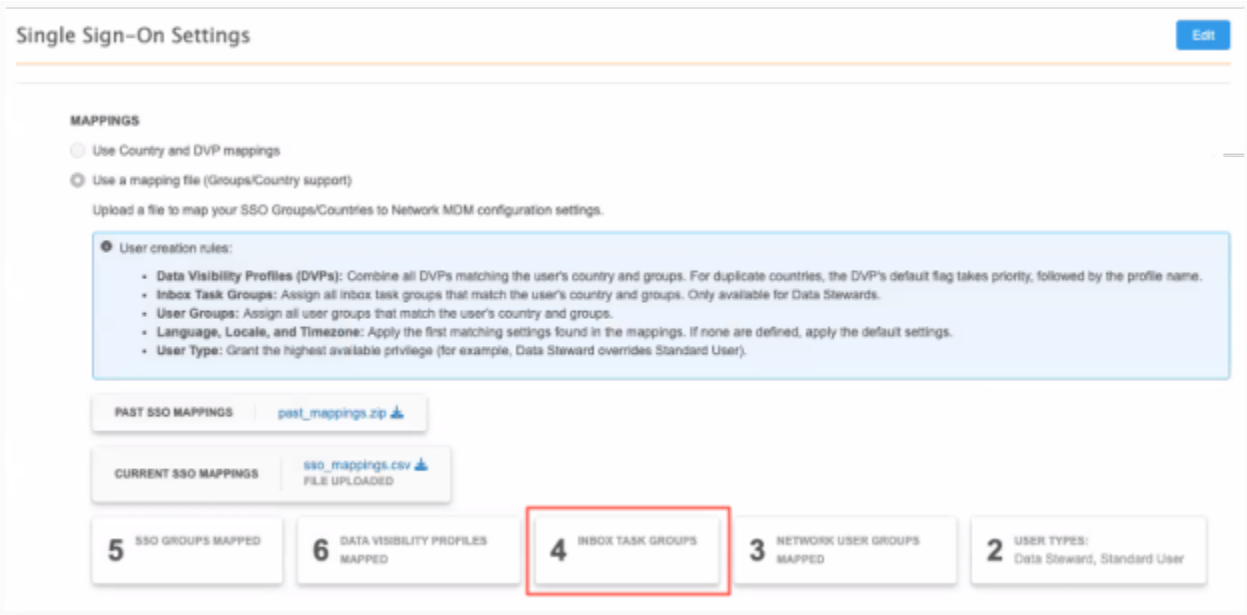
To continue using the package, clone it and remove the SSO settings.

Security

SINGLE SIGN-ON MAPPINGS

In version 26R2.0, single sign-on was enhanced to enable Administrators to use a mapping file to dynamically provision new users. This release expands those mappings to include Inbox Task Groups for Data Steward users.

Administrators no longer need to manually assign inbox task groups to each new data steward user. When data stewards log in for the first time, they can immediately access tasks assigned to the inbox task group.



This enhancement is enabled by default.

Supported user types

- Data Stewards

Inbox task groups cannot be assigned to Standard Users or Portal Users.

Mappings file

The `sso_mapping.csv` file is updated to include a column for Inbox Task Groups.

When the user type is Data Steward, add the required Inbox Task Groups using the inbox task group ID found in the `network_configurations.xlsx` file that is downloaded with the `sso_mappings.csv` file.

Multiple inbox task groups can be added as comma separated values.

Example

	A	B	C	D	E	F	G	H	I	J
1	SSO_GROUP	Group Info	SSO_COUNTRY	NETWORK_USER_TY	NETWORK_DVPS	NETWORK_USER_GRO	NETWORK_LOCALE	NETWORK_TIME	NETWORK_LANG	NETWORK_INBOX_TASK_GROUPS
2	91568a03-7e6	KAMs		DS	us_data__c		en_US	GMT	en	canada_ds__c;;data_stewards__c
3	377386619-23	data science		DS	turkey__c;;russia	Marketing_Users	es_MX	GMT	en	fr_ds__c
4	77386619-231	Developers		DS	us_data__c	Marketing_Users	es_MX	GMT	en	data_stewards__c;;us_prescribers__c
5	91b46b3e-051	albany_office			jersey__c	albany_office	es_MX	GMT	en	
6	04929562-ac2	Marketing					es_MX	GMT	en	
7										

Important: The user must have access to data for the Inbox Task Group country. Ensure that the data visibility profile (DVP) for that country is also assigned to the user type in the NETWORK_DVPS column.

Validating the mapping file

When you upload the file, the Inbox Task Group configurations are validated. Errors will occur for the following issues:

- Inbox task groups are assigned to Standard users or Portal users. Those user types do not have access to the Network MDM inbox.
- An unknown inbox task group was included.
- The Data Loading inbox task group was included. This inbox task group applies to Administrator and Data Manager users only. It cannot be assigned to Data Steward users.

Creating the user

When the file is successfully uploaded and the SSO configuration is saved, users logging in as Data stewards will be automatically created and assigned to the Inbox Task Group.

When they access your Network MDM instance for the first time, the Inbox page displays and includes the tasks for their assigned Inbox Task Group.

UPDATES TO TRANSPORT SECURITY LAYER CIPHERS

To ensure the highest security standards, the following TLS cipher will be removed from publicly accessible Network FTP servers.

- TLS_DHE_RSA_WITH_AES_256_CCM_8

While Network MDM already enforces TLS 1.2, retiring these ciphers eliminates known vulnerabilities and strengthens your data protection.

This change will be made by default.

Impact to existing customers

No disruption is expected. Standard FTP clients will automatically negotiate stronger, supported ciphers with no action required.

If you connect using older FTP clients or custom automation scripts, you might need to update your software to maintain connectivity.