Administrators Reference Guide

This guide is intended to be used by Vantiq administrators and covers how to authorize users to access a Vantiq installation and how (and why) to create Vantiq namespaces to perform development tasks and deploy applications. The organization of this guide is somewhat task oriented, but it is intended to serve as a reference guide. For a more directed introduction to the topics covered here please refer to the User and Namespace Administration Tutorial.

Concepts and Terminology

The following terms are used throughout this guide and it is assumed that the reader is familiar with them:

- **Organization** – a tenant of the Vantiq system to whom the system administrator has delegated the authority to manage both users and namespaces. See also the organizations resource.
- **Namespace** – defines an isolated environment for users of the Vantiq system. Each namespace guarantees separation of Projects, Apps, Collaboration Types and other Vantiq resources from all other namespaces. See also the namespaces resource. Namespaces can be placed into different categories, such as:
  - *System Namespace*: the namespace used to hold the resource instances defined by Vantiq (aka the *system* resources).
  - *Organization Namespace*: this is the root namespace for a Vantiq organization. It exists to hold organization-wide Vantiq resources, such as the users who are part of the organization and other resources that have meaning across the entire organization.
  - *Developer Namespace*: this is a namespace used by a Vantiq developer to hold the application resources that are under development. The namespace's collection of resources is loosely referred to as a Vantiq application. New users cannot be *created* in a developer namespace.
  - *Application Namespace*: this is a namespace used by the organization to hold the resources of a deployed Vantiq application. If needed, new users can be created specific to the application, homed in the application namespace. But new namespaces cannot be created while in an application namespace.
- **Vantiq User** (aka user) – an individual who has been authorized to access the Vantiq system. See also the users resource.
- **Privileges** (aka authorizations) – the set of operations that a user has been authorized to perform on specific resources. For purposes of this document we are mostly concerned with operations on namespaces and users. Privileges are assigned in the context of a namespace, so what a given user can do in one namespace might differ from what they can do in another. The following authorizations may be assigned to govern system resource access:
  - *Admin*: an Administrator has the ability to create, modify and delete (aka manage) Vantiq resources within the namespace. Depending on the specific type of admin they may also have the ability to manage namespaces and/or users.
  - *Developer*: a Developer is a special privilege level and may only be created in an organization namespace. Developers can manage all resources associated with creating Vantiq applications. Developers may create new namespaces for their development projects and may grant existing users access to those namespaces. However, Developers may not create new users.
  - *User*: a User has the ability to view but not manage Vantiq resources within the namespace.
- **System Administrator** (aka sys admin) – any user who has been given admin privileges in the system namespace. The sys admin can create new organizations and can authorize the initial organization admin.
- **Organization Admin** (aka org admin) – any user who has been given admin privileges in an organization namespace. The org admin can manage both the users and namespaces that are part of the organization.
- **Namespace Admin** – any user who has been given admin privileges in an application namespace. Namespace admins can create new users homed in the namespace and can authorize existing users to access the namespace. They may not create new namespaces.
  Namespace Admin privilege only exists in an *application* namespace (and not in a *developer* or *org* namespace).
- **User Admin** – a user who can create and revoke User-level and User Admin-level users, but otherwise has the same permissions as a User. User Admin privilege only exists in an *application* namespace (and not in a *developer* or *org* namespace).
- **Home Namespace** – the *home* namespace for a user is the namespace in which their users resource instance was created (every instance of every resource exists in one, and only one, namespace). A user must always have at least minimum privileges in their home namespace (these cannot be revoked). Deleting a user's home namespace will revoke all of the user's Vantiq authorizations.

Related Configuration

There are a few system configuration options that can influence exactly what the user sees when managing namespaces and users. While these are outside the scope of this document, we did want to highlight them so you are aware of their impact. In each case this document assumes that the configuration matches the configuration of the Vantiq cloud.

Authentication

Vantiq can be configured with one of 2 different authentication mechanisms – internal or OAuth. This choice is made at deployment time and cannot be changed without re-installing the Vantiq node from scratch. Vantiq recommends that central nodes be configured to use OAuth. The use of internal should be reserved for Vantiq edge nodes. How to configure these options is outside the scope of this document.

The choice of authentication option influences many of the tasks described in this document. Rather than discuss each option for all tasks, we will only cover the "internal" option for tasks that we expect to be performed on Vantiq edge nodes. Otherwise, it should be assumed we are using the OAuth configuration.

Sending Invitations

Many of the authorization tasks described in this document involve having Vantiq send an "invitation" to the person who will complete the task. By default these invitations are sent using the `GenericEmailSender` source which is part of the default Vantiq configuration. In the Vantiq cloud, this source is configured to send email from Vantiq Operations. It is also possible to send invitations using either an EMail or SMS source defined in the local namespace. When using an SMS source, you will use the user's phone number and not their email address.
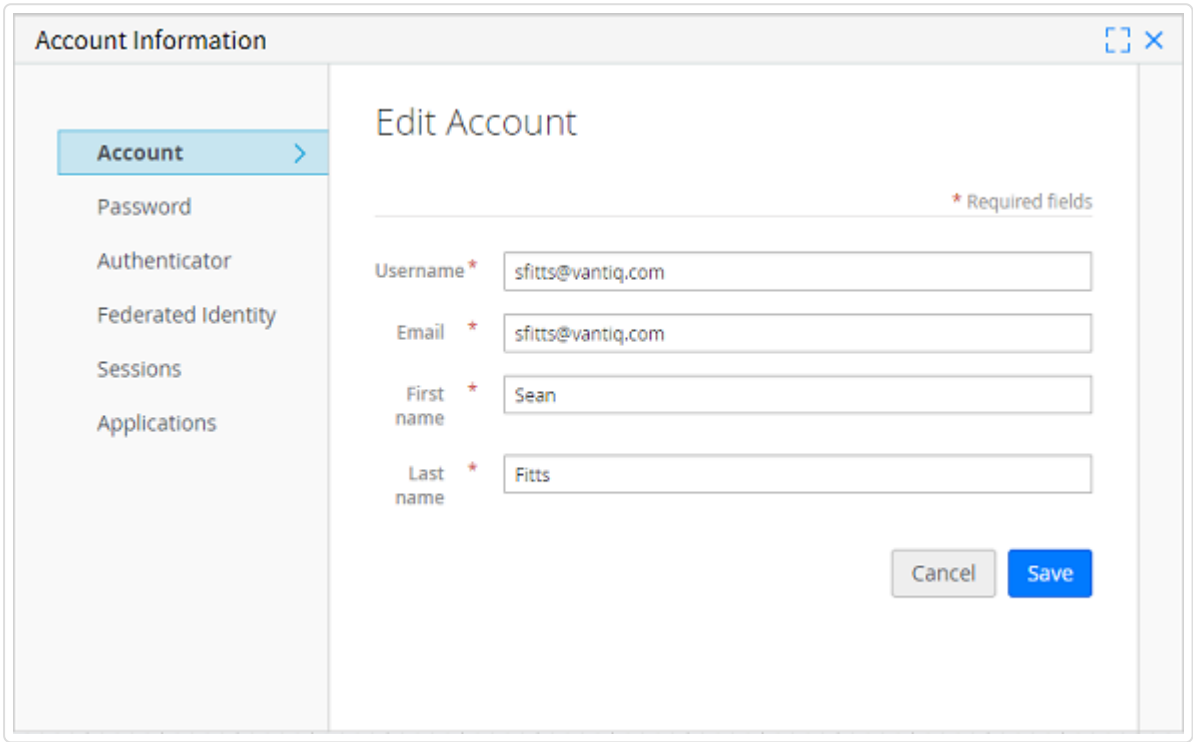
Self-Administration Tasks

Update Account Info

When configured for OAuth, Vantiq delegates management of all user profile information to the OAuth provider. For the Vantiq cloud based systems, that provider is [Keycloak](). To access the user profile, bring up the "user info pop-up" by clicking on the user's name in the upper right hand corner of the IDE:
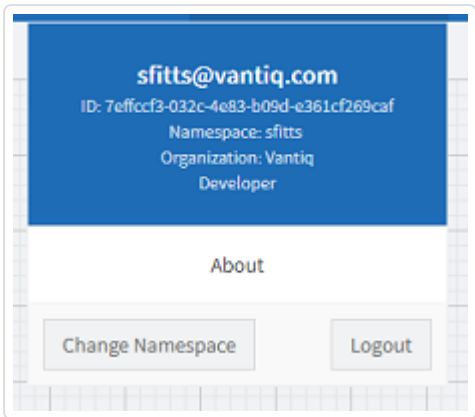
From there click on the user name at the top to launch the Account Information pane:

From here the user can update their preferred username, add a Vantiq specific password, link to other OAuth providers, and configure multi-factor authentication.

System Administration Tasks

Authorizing the Initial System Admin

The initial sys admin should be established immediately after deploying a new Vantiq node. How this is done depends on how the node is configured to perform authentication.

Internal Authentication

The initial sys admin is created as the well-known user `system` with a default password of `fxtrt$1492`. The password should be changed immediately after deployment, before the Vantiq node is made available to any other user.

OAuth Authentication

When the Vantiq server is started for the first time, it will print an authorization code to its log file (this code will only be printed once, so it should be recorded immediately). Here is an example of the code:

Once the code has been recorded the intended sys admin should navigate to the root URI for the Vantiq node. This will trigger authentication via the configured OAuth system and then will present a page where the authorization code can be entered:
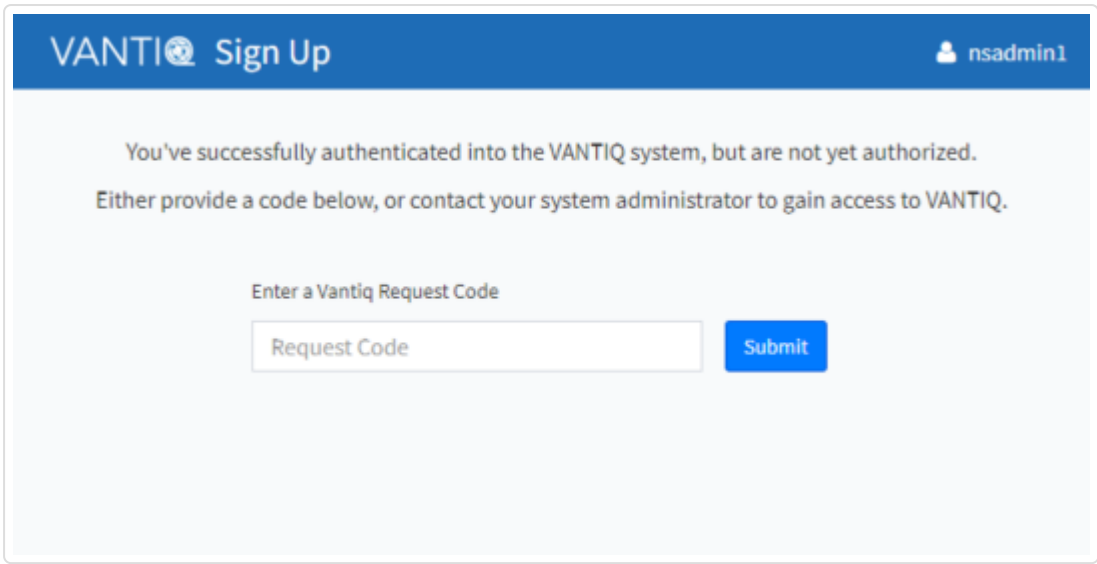
Submitting the correct code will result in the user being authorized as the sys admin.

Creating a New Organization

To create a new organization open the organizations pane using **Administer** > **Organizations**, and click the `+ New` item just under the title. This will bring up the following editor:

From this editor, you configure the organization you wish to create. The top section allows you to provide details about the organization itself. Specifically, you give the organization a name, a description, and can specify the various properties below.

- **Is Isolated** – whether the organization runs in a set of isolated servers
- **Enable Monitoring** – whether to monitor the operation of the organization
- **Monitoring Configuration** – allows you to override the default configuration
- **Quota** – allows you to override the default quota for organizations
  - The Quota editor is a JSON editor. It allows you to provide quotas for the various limits, rates, and credits applicable to Vantiq operations within that organization. For full details on how quotas are managed, see the [Workload Management guide](#).
  - `limits`
    - `minimumScheduledProcedureInterval` – lower bound for the interval of a scheduled procedure. This is an interval string (e.g.: "10 minutes"), and defaults to "1 minute".
    - `k8sResources` – limits on usage of K8s Resources belonging to the Vantiq cluster (*aka* `self`). If this limit is not provided, no usage is permitted. This limit is not provided by default. All values are specified as strings and are formatted according to the Kubernetes Resource Quantity rules. See [Kubernetes Resource Units](#) for details.
      Note: Using these settings requires the cloud to be configured with a k8sworker process running. Do not specify this setting if that is not configured. See the [External Lifecycle Management Guide](#) for more details on the K8s Worker.
      - `vCPU` – the number of CPUs an organization can consume
      - `memory` – the amount of memory an organization can consume (in bytes, e.g 100M or 3G)
      - `gpuAmd` – the number of AMD GPUs an organization can consume
      - `gpuNvidia` – the number of NVidia GPUs an organization can consume

- Note that these values are ultimately limited by the resources allowed by the Kubernetes system on which it is based. These quotas should be determined with consultation from the Kubernetes system administrator.
      - `documentExpansion` – limits on the amount of memory that can be consumed for processing large objects (often, but not limited to, images) in the server. This is used to limit an organization's storage of temporary images (the results from the VIDEO source) as well as that used for sending large amounts of data (see Document, Image or Video Operations). The default is 0.
    - `credits` – for details, see the Workload Management guide
    - `rates` – for details, see the Workload Management guide
  - **Configure Products** – configure the products users of this organization are allowed to use
  - **Namespace** – the name of the organization namespace for this organization.

The bottom section allows you to configure the organization namespace that will be created as part of creating this organization.
See the section(s) on creating namespaces for more details, but, generally, from here you can choose to either make yourself the administrator of the new organization or you can choose to invite someone else to take on that role. In the latter case you will enter the email address of the person you wish to invite. When that person receives the email it will include a link which, when followed, will authorize them to be the organization admin. This person may or may not already be a Vantiq user. If they are not, then processing the invitation will result in creating a new user with the organization namespace as its home. If the user already exists, then processing the invitation will add the necessary privileges to that existing instance.

Creating Resources for New Organizations

System admins can setup resources to be automatically installed into every new org namespace. The resources are specified through a document that is a zip containing an export of the resources.

The document must be named `org/newOrganizationResources.zip` and must be in the system namespace. That zip file will be imported into the new org namespace, and will include all the resources and data contained within. It should be formatted in the same manner as an export from the UI or CLI. For the latter, you'll need to place all the exported folders in the top level of the zip file.

Updating the URI

If the Vantiq installation's URI changes, any nodes that were pointing to it will fail to connect. An operation is provided that will update all nodes in all local namespaces, and may try to update them in remote installations as well.

Operation Format

This is an operation on the nodes resource, no resourceId required. The operation name is `updateUri` and it accepts an object with two fields:

- **oldUri** – The URI to be replaced.
- **newUri** – The URI that **oldUri** should be changed to.

If using the REST API you send a POST request to `api/v<version>/resources/nodes/updateUri`, and the body's format is

```
{
    "operation": "updateUri",
    "data": {
        "oldUri": <value>,
        "newUri": <value>
    }
}
```

What it does

When you run the operation, it will replace `oldUri` with `newUri` in uri related fields for each node, node configuration, and deploy configuration in any namespace on the local installation.

If `oldUri` is the `uri` value for the self node in the system namespace it will also try to fix remote resources too. Every local node will try to perform the same changes in their connected namespace, and every catalog member will update the uris for member-to-member connections pointing to them.

In each case, it doesn't replace URI prefixes. For example if you're updating the URI from "http://my.vantiq.com" to "https://your.vantiq.com" and you have a node with the URI "ws://my.vantiq.com", it will change that node's URI to "ws://your.vantiq.com".

Organization Administration Tasks

Adding a New User to an Organization

To add a new user to an organization open the users pane using **Administer** > **Users**, and click the `+` icon in the title bar. This will bring up the new user editor:

Enter the email address of the person you wish to add to the organization. By default the user will be assigned the "User" privilege level. You may or may not want to change this depending on what role the user will play within the organization. The potential roles are:

- Organization Admin – in this case you will want to grant the "Organization Admin" privilege level.
- Developer – in this case you will want to grant the "Developer" privilege level. You can also specify a namespace to be created for the user at the same time.
- Application Admin – in this case you will want to grant the "Namespace Admin" privilege level.
- User Admin – in this case you will want to grant the "User Admin" privilege level.
- Application User – in this case the default permission is sufficient.

If you decide you want to use a non-default authorization for the user, click on the "pencil" icon next to `Authorizations` . This will bring up the following sub-editor:

This will let you change the authorization for the organization namespace. You can also use this to add authorizations to other, existing namespaces, which can be useful when adding a new application admin or user for an already existing application.

Custom User Invites

Vantiq's default user invitation is barebones: a short paragraph stating that you've been invited to namespace X on installation Y, with an acceptance link and an expiration date. The user invite template can be changed by creating specific Documents in any of three locations:

- `invites/newUserInvite.html` in the system namespace – This sets the default for the entire installation.
- `invites/org/newUserInvite.html` in an Organization namespace – This sets the default for the entire Organization, and overrides the system default.
- `invites/local/newUserInvite.html` in any namespace – This sets the default for the specific namespace, and overrides the system and Organization defaults.

Note that the template is selected based on the namespace the invitation is sent from, not the namespace the invitation is for. Additionally, if you are creating the invitation programmatically instead of through the UI, you can specify other templates in the request. See namespaces and delegated request docs for more detail.

You may also customize the email's subject line, both at creation and when sending the message.

Template Formatting

Templates are HTML files with parameters that can be filled in when the invitation is sent. After being filled in with the parameters, they are sent in an email to the specified address.

Custom parameters are created by placing `${myParameter}` in the template, and when the invite is sent they will be replaced by the provided value. There are also four parameters always provided by the server. Their inclusion is generally optional, and they're listed below.

- `acceptUri` – The URL used to accept the invitation. **This is required for the recipient to gain access to namespaces and the installation.**
- `expirationDate` – The time the invitation expires.
  Here's an example of the way it's formatted `Wed, 21 Dec 2022 10:16:03 −0800`.
- `p0` – The username of the user creating the invitation.
- `p1` – The namespace the recipient is being invited to.

Here is an example template:

```
Hello ${inviteeName},

You have been invited to namespace ${p1} by ${companyName} because ${reason}.

<a href="${acceptUri}">Click here to accept</a>

Thank you,
${companyName}
```

When the above is the default template for a namespace, the Administer>Users>New pane will look as below. The custom parameters can be filled in for each invitation, and the server provided parameters will be added when the invite is sent.

Deploying the GenAI Flow Service Connector

In order to use the GenAI Flow Builder you will first need to deploy the GenAI Flow Service Connector for your organization. This is done by importing the GenAIFlowService project into the organization namespace. Once imported, the connector will be deployed via the Vantiq K8s infrastructure.

> Note: deploying the service connector requires `k8sResources` quota for the organization; contact Vantiq support if that does not exist in your organization. Details on the k8sResources quota is under Quota in the Administrators Reference Guide. If enabled, the current *K8s Resource Usage* can be seen using the Administer -> Organization menu when in the organization namespace.

Deploying the Video Assistant Service Connector

In order to use a VIDEO source you will first need to deploy the Video Assistant Service Connector for your organization. This is done by importing the VideoAssistant project into the organization namespace. Once imported, the connector will be deployed via the Vantiq K8s infrastructure.

Note: deploying the service connector requires `k8sResources` quota for the organization; contact Vantiq support if that does not exist in your organization. Details on the k8sResources quota is under Quota in the Administrators Reference Guide. If enabled, the current *K8s Resource Usage* can be seen using the Administer -> Organization menu when in the organization namespace.

Also, the use of a Video source requires `documentExpansion` quota for the organization; contact Vantiq support if that does not exist in your organization. Details on the `documentExpansion` quota is under Quota in the Administrators Reference Guide.

Creating a New Application Namespace

To deploy a Vantiq application in the organization, the org admin will need to create a new namespace to contain the application's resources. This is known as an *application namespace*. Before creating the namespace make sure you know who you intend to act as the namespace admin. There are 3 options:

- The org admin – in this case the org admin will also be taking on responsibility for managing the new application.
- An existing org user – this is the typical case when managing an application used by users who belong to the organization. In this case you want to be sure that the user has been added to the organization before creating the namespace.
- A new user – this option should only be used when the application will be used primarily by users who are not part of the current organization.

To create a new application namespace open the namespaces pane using **Administer** > **Namespaces**, and click the `+` icon in the title bar. This will bring up the following editor:

Set the "Authorization Level" to `Namespace Admin` and choose who to authorize. When creating the new namespace the org admin can choose to either make themselves the namespace admin or delegate that privilege to another user. To authorize another user as a namespace admin, enter their email and send them an invitation. In most cases the user you choose should already have been added to the organization as described in the previous task. The only exception to this is if the application that will be deployed in the namespace will be used by users outside the current organization.

Creating Resources for New Namespaces

Org admins can setup resources to be automatically installed into every new namespace created in that org. The resources can be specified in two different ways:

- upload a document that is a zip containing an export of the resources OR
- put the resources into a specific project in the org namespace.

The document must be named `org/newNamespaceResources.zip`. It will be imported into the new namespace, and will include all the resources and data contained within. It should be formatted in the same manner as an export from the UI or CLI. For the latter, you'll need to place all the exported folders in the top level of the zip file.

The project must be named `newNamespaceResources`. All resources in the project will be imported, including the project definition. You can also import data by making the project an assembly and setting the `selectData` field as if publishing the assembly.

If both are specified then both will be imported, with the zip file fully imported before the project.

Creating a Developer Namespace for the Organization Administrator

Sometimes the org admin will also want to do Vantiq development work. In this case they should create a developer namespace in which to do the work (and from which they can create other developer namespaces). To do this open the namespaces pane, and click the `+` icon in the title bar. This will bring up the new namespace editor as in the previous task. At this point set the "Authorization Level" to `Developer` and check the `Make Me The Administrator` checkbox, like so:

This will create a new developer namespace owned by the org admin.

Accessing Namespaces in the Organization

Org admins can always give themselves access to any namespace in their organization. However, doing so will clutter their profile list and several screens in the UI. Instead of doing this, the org admin can set the parameter `asOrgAdmin` to `true` for requests to any namespace in their organization. This option will let them act as if they were an admin in the namespace, and it is limited to the following operations:

- Select and Select One
- Aggregate
- Upload
- Insert
- Upsert
- Update
- Patch
- Delete
- Publish to topics, service events, or sources
- Execute procedures
- Get Authorized Users

This does not override explicit permissions. If an org admin uses this option on a namespace where they have user-level permissions, then they will use the user-level permissions for that action.

For REST requests, the option is applied as a query parameter in the url. For WebSockets and VAIL, it should be an entry in the `parameters` object.

When using tokens, e.g. for external REST requests, the token must be a full(non-single-namespace) personal token for the org administrator. The token used by the UI works as well.

Sample VAIL for asOrgAdmin

The below code will perform a Select One operation in another namespace. It will succeed if either:

- The user running the code is an org admin in the org containing the target namespace and is using a full personal token, or
- The user running the code is authorized in the target namespace.

```
var op = {
    op: "selectOne",
    resourceName: "system.namespaces",
    parameters: {
        where: {namespace: {ars_substitution: "ars_currentNamespace"}},
        props: ["namespace", "organizationRef", "ars_properties", "ars_createdBy", "ars_createdAt"],
        asOrgAdmin: true
    },
    targetNamespace: "exampleNamespaceName"
}
ResourceAPI.executeOp(op)
```

Active Resource Control Center

The Active Resource Control Center allows you to see all activatable resources in a namespace and easily change their activation status. When in an org namespace, you can do the same for all namespaces in that org.

It shows all the apps, services, events, sources, and rules in the namespace. For each of these, it gives the name and activation status. Clicking on the toggle in the right-hand column will change the activation status of the resource, with blue meaning active and gray meaning inactive.
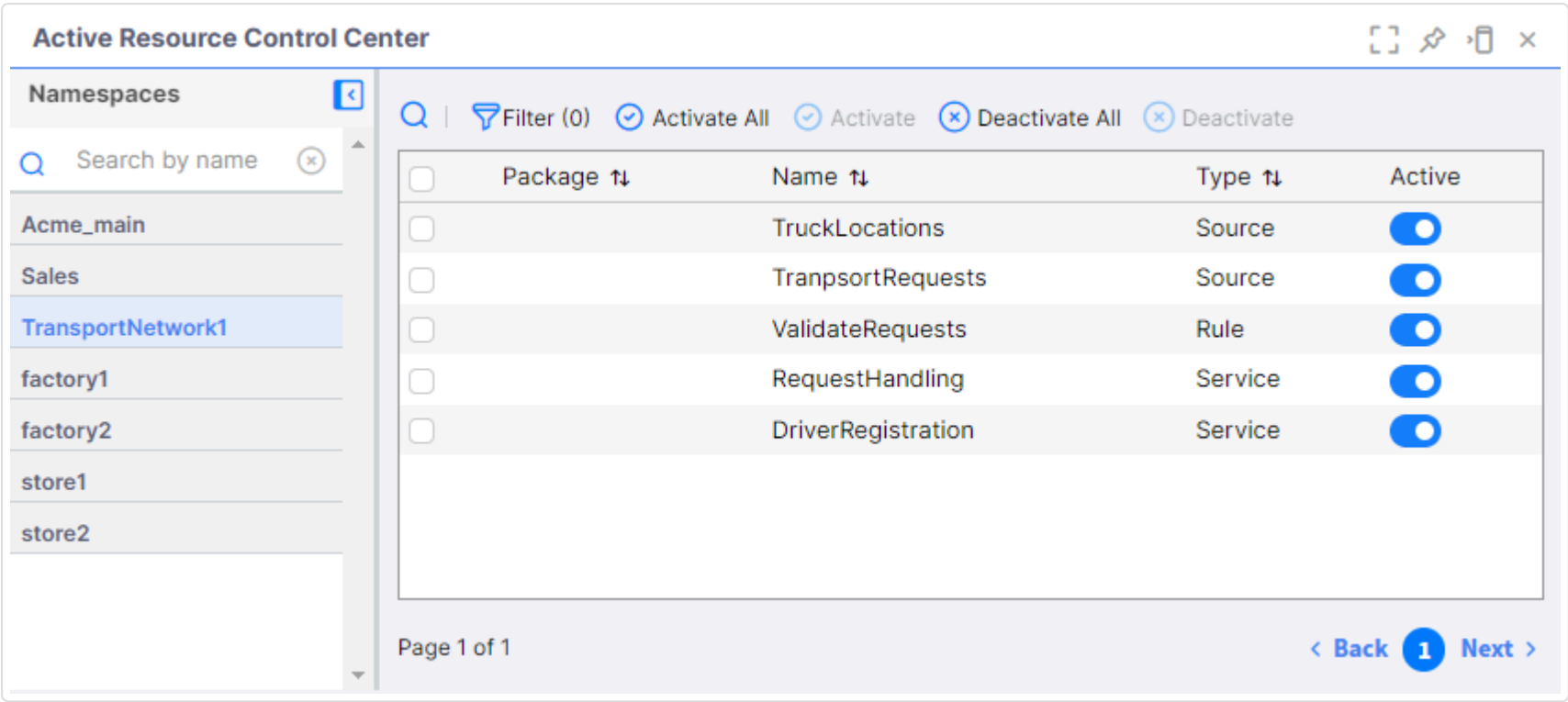

Note that this will not work for namespaces where you only have user-level permissions.

Removing Namespace Administrators

Sometimes you will need to remove users from your organization. If they are admins in any namespaces, simply revoking their access may result in applications in those namespaces not working correctly. Tokens they created will be deleted, groups they own can no longer be edited, and rules and apps they worked on may no longer run.

To avoid this, you should use the pane `Administer` > `Advanced` > `Revoke Access`. Here you will be able to revoke users from multiple namespaces at once and transfer the relevant resources to yourself in each namespace. The user will only lose access to the checked namespaces. This may cause a temporary disruption in rules and apps, but the applications will continue to function afterwards.
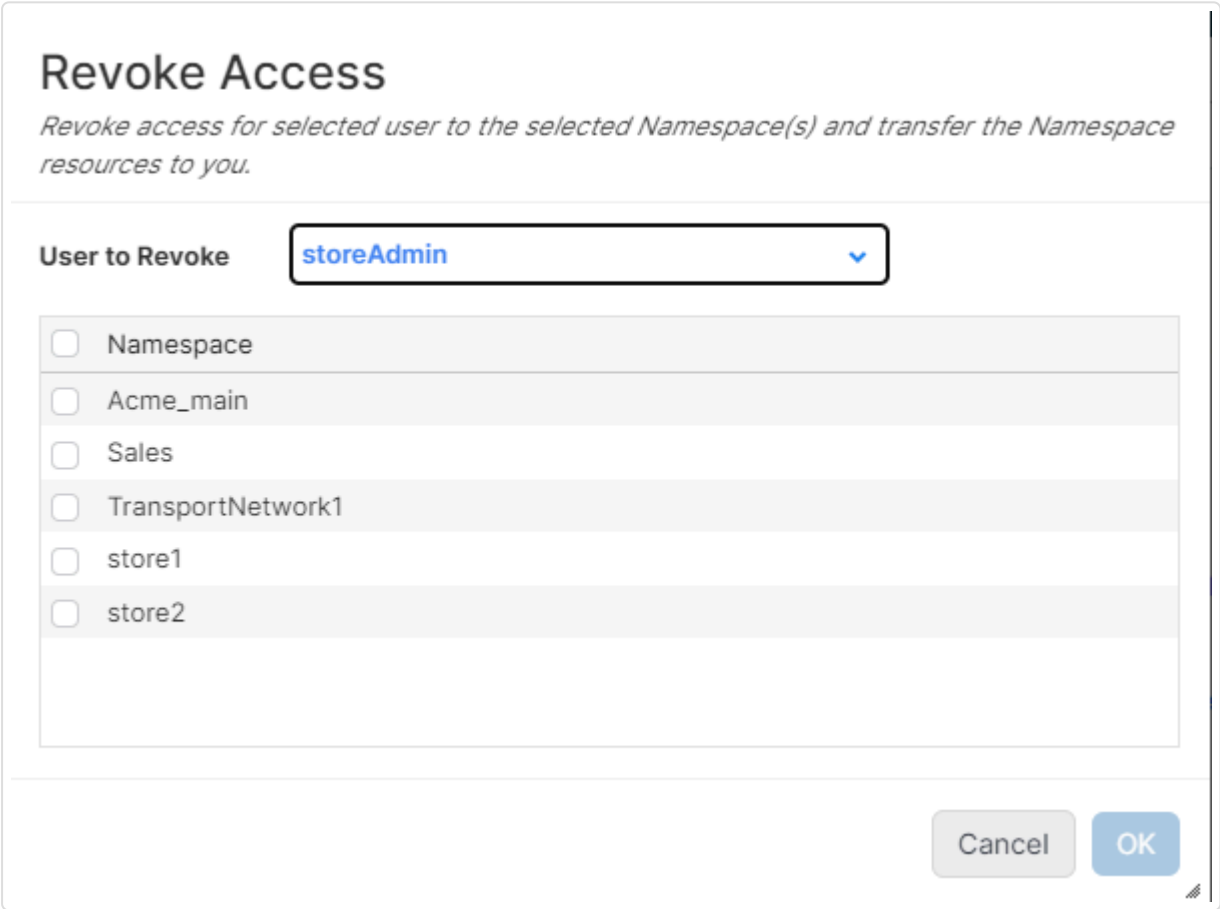
The specifics of what will be transferred and how can be found here.

Note that you will be unable to do this for the user's home namespace. You cannot use revocation to remove a user from their home namespace, and instead must delete them there.
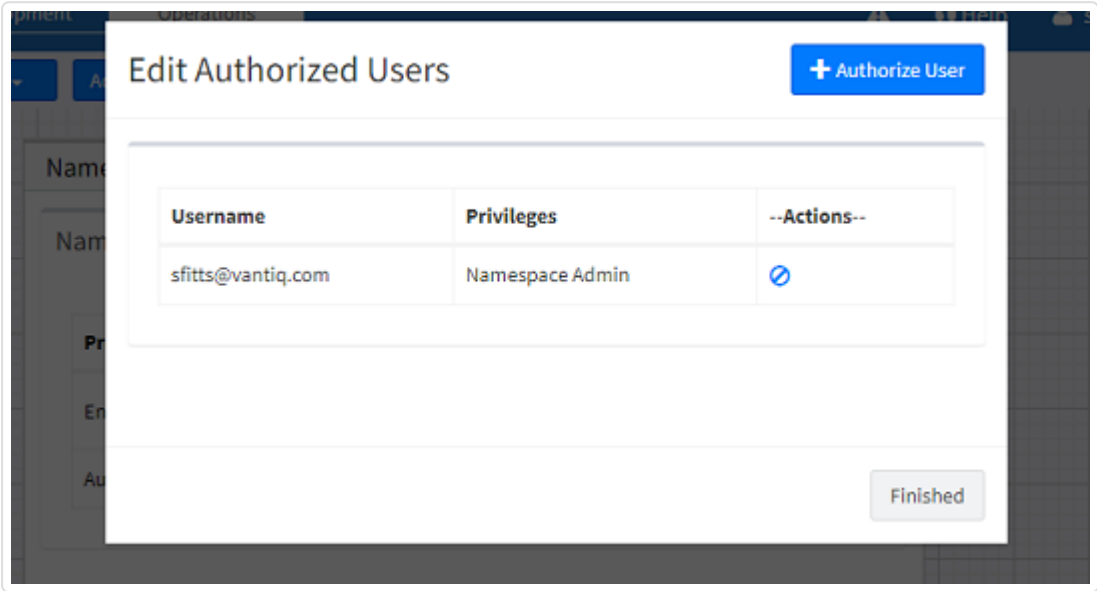
Application Administration Tasks
## Authorizing Users to Access the Application

To authorize a user to access the application, open the namespaces pane, click on the namespace to bring up the namespace editor:
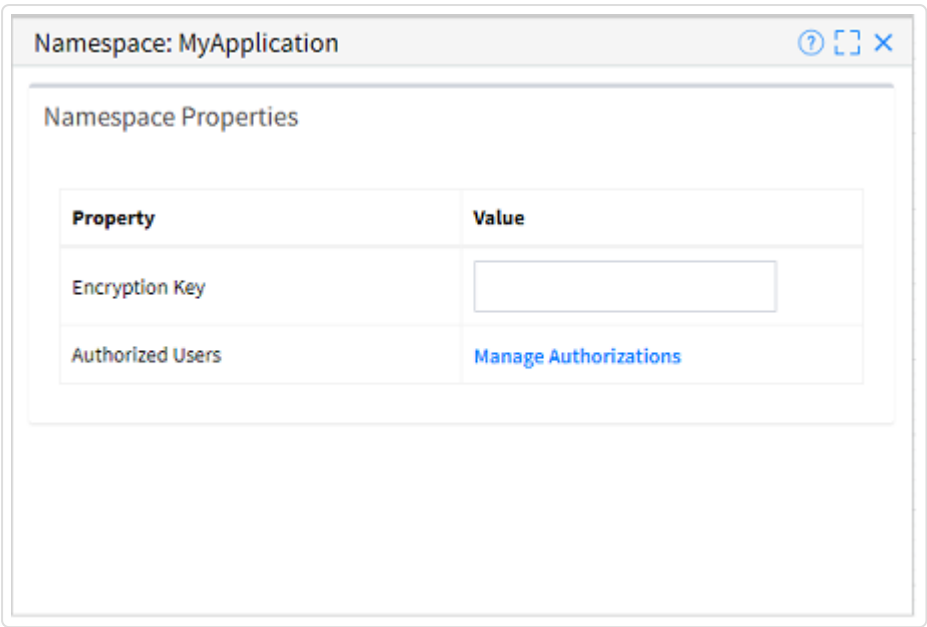
From here click on `Manage Authorizations` to bring up the Edit Authorized User dialog:

This shows all users current authorized in the namespace and their current privileges. To authorize an additional user, click on `Authorize User` which will bring up the Send Invite dialog:
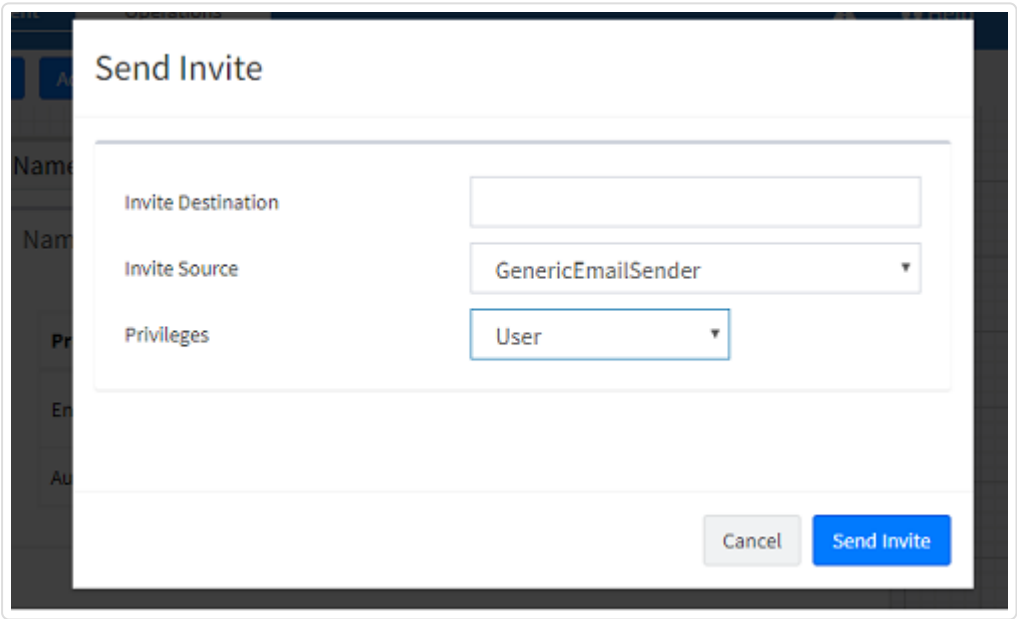
Here you can provide the user's email and select what privileges to grant them. For an application namespace you can choose to grant the `User` , `User Admin` , or `Namespace Admin` privileges. Additionally, if your application includes custom profiles then `Custom` will also be an available choice.

Adding a New User to the Application Namespace

When managing an application being used by users who are not part of the organization, it can sometimes make sense to add these users directly to the application's namespace. Remember that in doing this, the application namespace becomes the *home* namespace for these users. This means that if the application namespace is deleted, those users will lose all of their Vantiq authorizations (which may or may not be what you want).

To add a new user to an application namespace, open the users pane, and click the `+` icon in the title bar. This will bring up the new user editor:

By default the new user will have the `User` authorization level.

If you decide you want to use a non-default authorization for the user, click on the "pencil" icon next to `Authorizations`. This will bring up the following sub-editor:

Here you can choose the privileges to grant – `User`, `User Admin`, `Namespace Admin`, and possibly `Custom` (if there are non-default profiles available).

Viewing Lists of Users

When administering a namespace there are two views of users that an administrator may need. The first is the list of users who are homed in the namespace. These users were first created in this namespace, and deleting this namespace will completely remove the user and revoke their access to all authorized namespaces. This list can be found under `Administer` > `Users`.
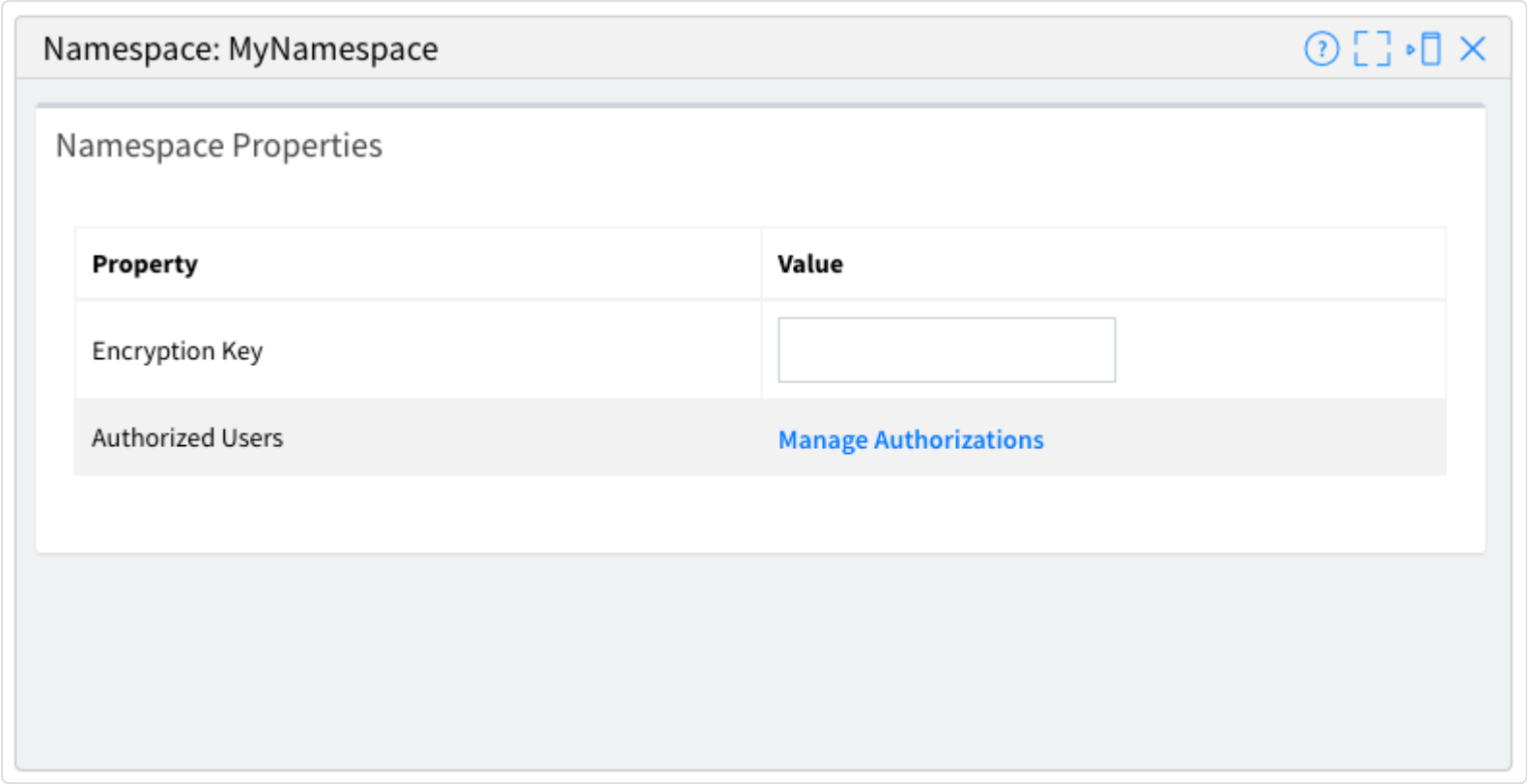
Separately, it's possible to view a list of all users authorized in a namespace. These users may or may not be homed in the namespace, but they all have profiles granting some access to the namespace. Start by opening the namespace detail pane by first going to the namespaces list under `Administer` > `Namespaces` and clicking on a namespace in the list:

The list of users authorized in the namespace is found by clicking the `Manage Authorizations` link, which opens the following popup:
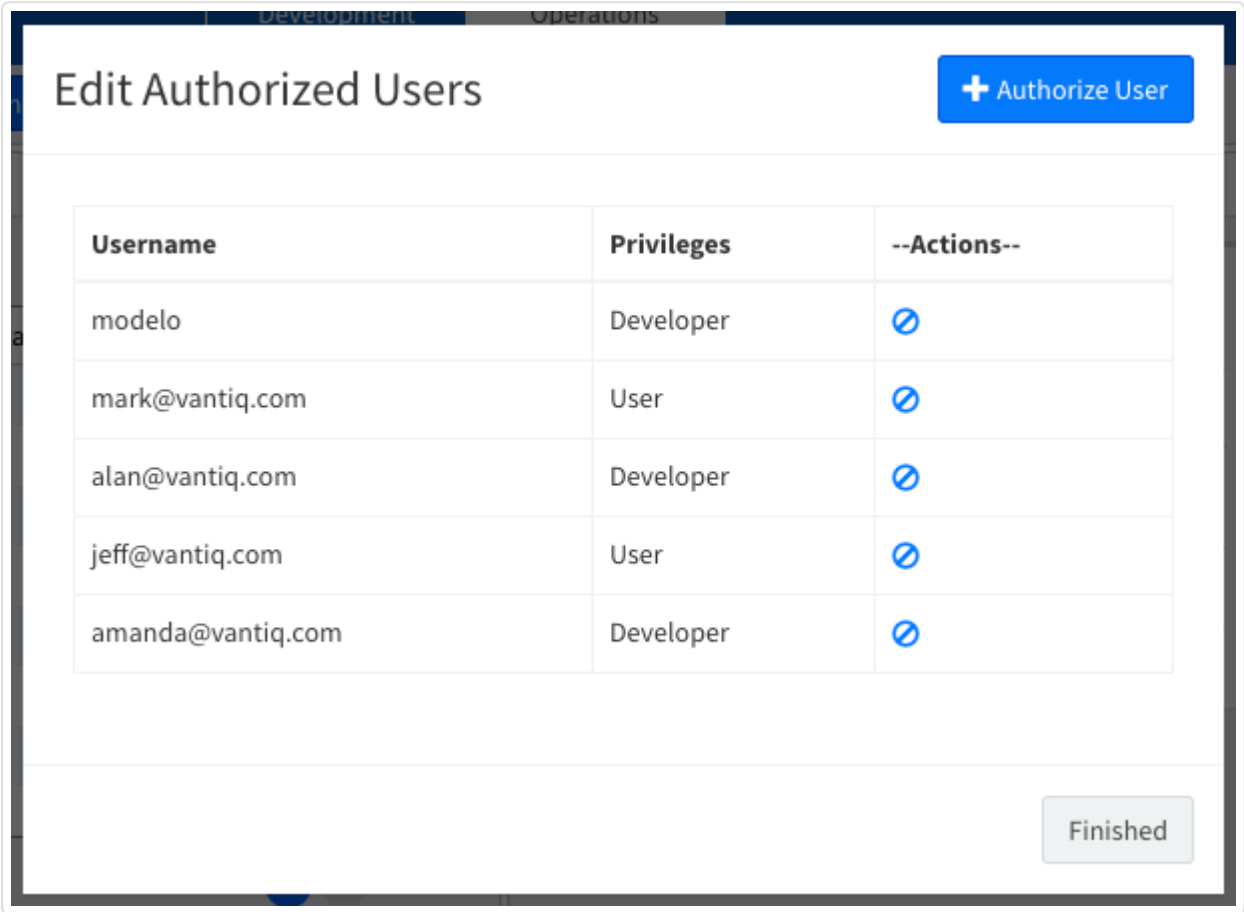
Handling Administrators Leaving

When administrators leave a namespace, they can leave behind resources that will not function without them. For example, rules they created may start throwing authorization errors, since rules use their author's permissions. If you are in charge of revoking them, you can claim these resources when you perform the revocation. If they have already left the namespace, you can check for and claim their orphaned resources.

Claiming Resources on Revocation

It is best to claim the resources on revocation. This minimizes the interruption to rules and apps and preserves non-personal tokens.

To do this, you must remove the authorizations through the namespace administration pane. First, select `Administer` > `Namespaces` , then Edit the namespace to open its pane. Click on `Manage Authorizations` in the namespace pane. Once the popup appears, click the remove authorizations button for the desired user. You will be asked to confirm the de-authorization then asked if you want to transfer resources to yourself. Clicking Yes on both popups will revoke the user and claim certain owned resources for yourself. See here for details on what resources will be claimed and how.

Transferring Resources after Revocation

If a user has already left a namespace, you can still claim any resources they left behind. Note that tokens they created will have already been deleted, potentially causing problems with catalogs and remote nodes.

You can see if there are any orphaned resources in the namespace in `Administer` > `Namespaces` > the namespace. If there are any, the Transfer Resources row will be visible and you can manage the transfers.

Clicking "Manage Transfers" will open up a pane listing the usernames of all users with orphaned resources in the namespace. You can click to claim the resources from any of those users. Note that this will show the true usernames, which may not be the human-friendly ones displayed in most areas.

Developer Tasks

Creating a New Development Namespace

Whenever a Vantiq developer needs to work on a new application or on updates to an existing application they should create themselves a new namespace in which to do the work. Each namespace provides an isolated environment in which the developer can work without fear of having their work collide with that of another developer. To create a new namespace the developer should open the namespaces pane, and click the `+` icon in the title bar. This will bring up the following editor:
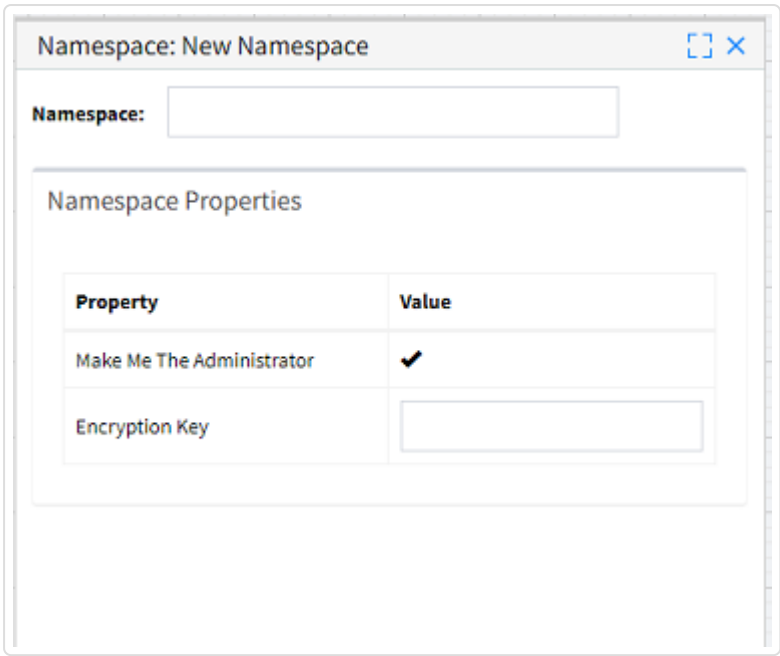
As a developer, the only choice for who to make the admin of the new namespace is the developer themselves, so this is the option that will be chosen.

Authorizing Other Users to Access A Development Namespace

There will be times when a developer needs to let other users access the contents of one of their namespaces. This could be to allow someone to test or preview a new feature that they are working on or in order to get help or feedback from another developer. This involves granting authorization to the other user (who must already be an existing Vantiq user) to a specific namespace. Start by opening the namespaces pane, and click on the namespace to be authorized. This will bring up the namespace editor:
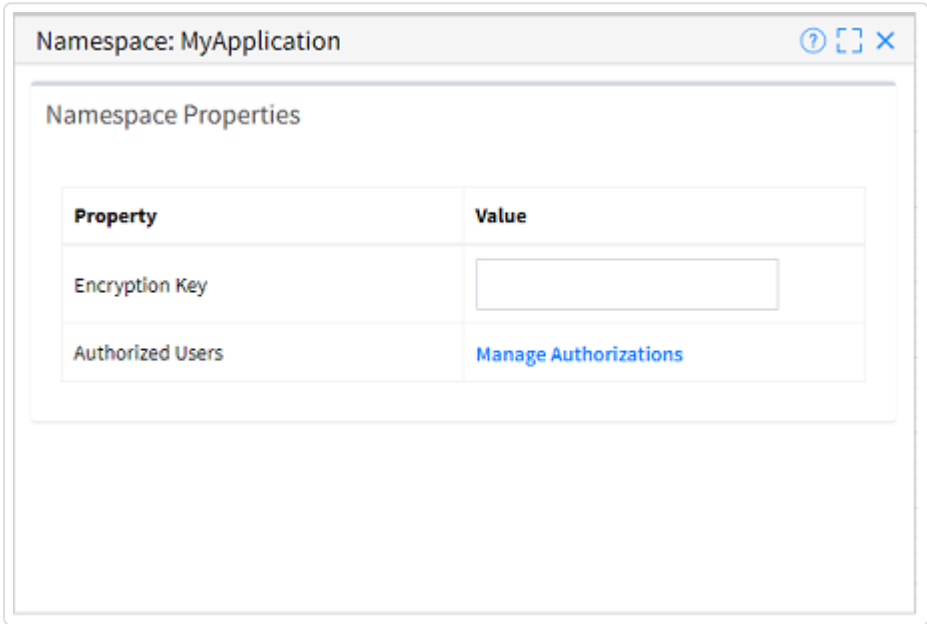
To authorize an additional user, click on `Authorize User` which will bring up the Send Invite dialog:
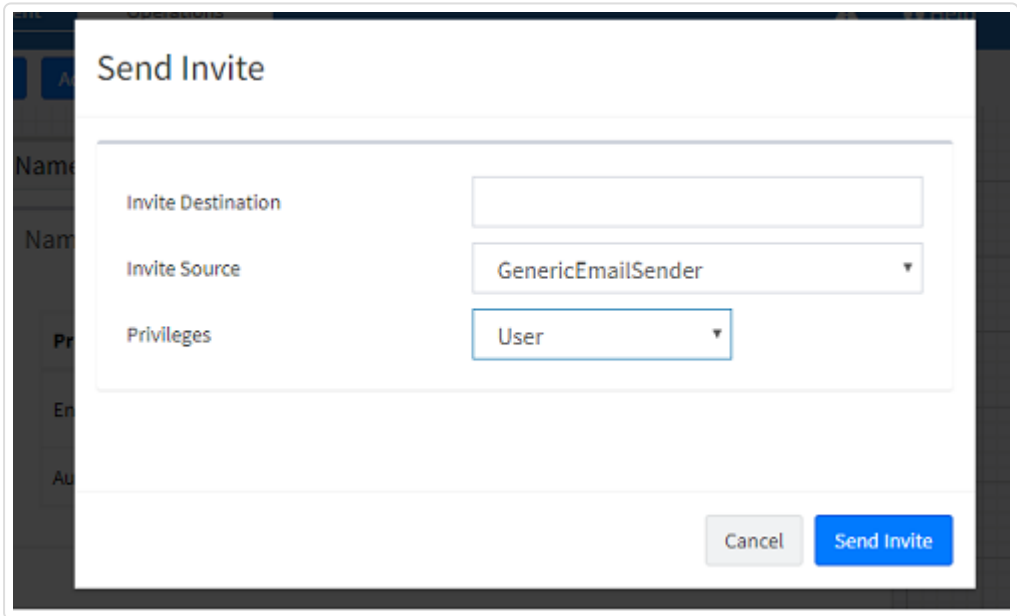
For a developer namespace you can choose to grant either `User` or `Developer` privileges. Additionally, if your namespace includes custom profiles then `Custom` will also be an available choice.

Handling Administrators Leaving

When administrators leave a namespace, they can leave behind resources that will not function without them. See the section for application admins for more details on how to properly handle this situation. Note that only the namespace owner can perform transfers in a development namespace.