Forcepoint Data Security Posture Management

Powered by Getvisibility

FDC Server Installation Guide

Report

Forcepoint
April 23, 2024

forcepoint.com

Table of Contents

PREREQUISITES 2
K3S INSTALLATION 2
RANCHER 3
KEYCLOAK 5
Logging into Keycloak Admin Panel 5
Completing the Realm Configuration 6
Completing the Dashboard Client Configuration 8
(Required for FDC/(FDC+FDV)) Setting Up a Default Agent User 9
(Optional) Completing the Agent Client Configuration 12
Creating a User to Access the Getvisibility Dashboard 13

Prerequisites

A VM or server with the following specifications:

- 8 x CPU cores (x86_64 processor with speed of 2.2 GHz or more). The CPU must support the instructions SSE4.1 SSE4.2 AVX AVX2 FMA
- 32GB RAM
- 500GB Free SSD disk. K3s will be installed in /var/lib/rancher so space should be allocated there. We also need 10-20 GB free space at / and /var.
- Ubuntu 20.04 LTS Server OS is recommended. RHEL 8.6, 8.7, 8.8, & 9.2, and Suse Linux 15.3 are also supported but may need extra configuration.
- Port 443/TCP open
- Outbound internet access to download application artefacts. 100 Mbps download speed recommended
- Domain Name Service (DNS) with public name resolution enabled
- Network Time Protocol (NTP)
- Software Update Service - access to a network-based repository for software update packages.
- Fixed private IPv4 address
- Unique static hostname

K3s Installation

From the command line of your chosen server, apply the following commands as root.

- This command instals K3s as well as checks the prerequisites:

  ```
  curl -sfL https://assets.master.k3s.getvisibility.com/k3s/k3s.sh |
  INSTALL_K3S_VERSION="v1.26.10+k3s1" K3S_KUBECONFIG_MODE="644" sh -s - server --node-
  name=local-01
  ```

- Once complete, copy the cURL command you received when registering the deal. It will look something like this:

  ```
  read -p "Please type your email address: " user_email && kubectl apply -f
  https://rancher.forcepointemea.k3s.getvisibility.com/v3/import/8wc8b6dnb9xvlh7grcrjpdwh55nc
  st2s9fqm96kt8zhc2k2stm7vck_c-m-6skspsgh.yaml && curl -k --location "https://customer-
  management.master.k3s.getvisibility.com/v1/updateClusterState/40093321-a4e2-4fe2-9493-
  36dc4b2ba7ab?email=$user_email"
  ```

  ⚠ Make sure to enter your email address to correctly install the platform and register with our customer service.

  For security reasons the registration command can be used only a single time, the command becomes invalid after the first use. In case you need to run it again you must contact the support team for a new registration command.

- To monitor the progress of the installation, enter the following command:

  ```
  watch -c "kubectl get deployments -A"
  ```

  The K3s deployment is complete when elements of all the deployments (coredns, local-path-provisioner, metrics-server, traefik and cattle-cluster-agent) show at least "1" as "AVAILABLE"

- In case of errors, you can inspect the logs of a pod using kubectl logs , e.g.

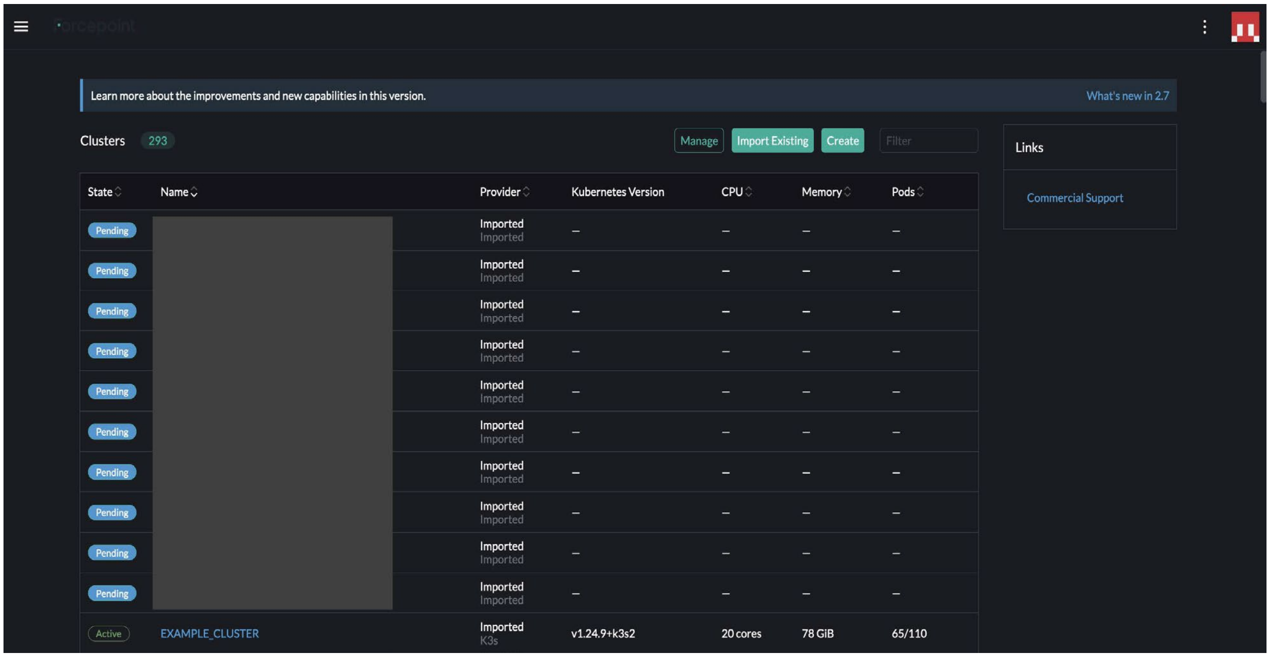
  ```
  kubectl logs cattle-cluster-agent-d96d648d8-wjvl9 -n cattle-system
  ```

  When installation is complete go to the rancher site associated with your region.

Rancher

The region and cluster name can be found in the registration email that was sent to you when you registered the deal.

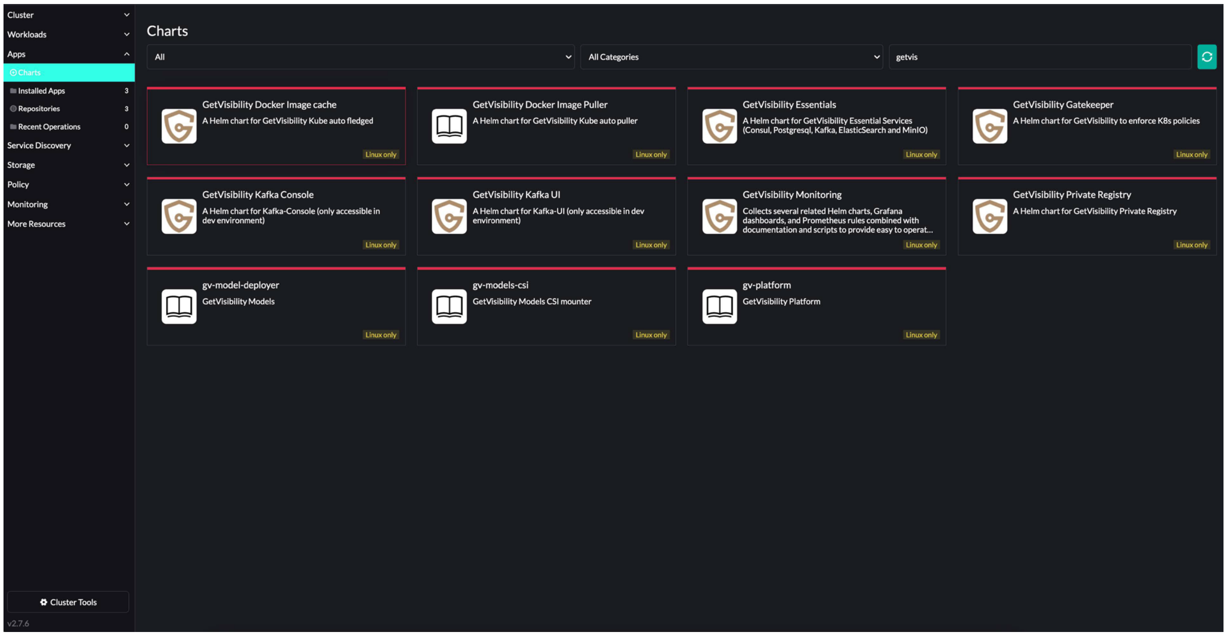
1. Go to your regional **Rancher** dashboard and wait for the new cluster to become **Active**.



State	Name	Provider	Kubernetes Version	CPU	Memory	Pods
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Pending	[redacted]	Imported Imported	–	–	–	–
Active	EXAMPLE_CLUSTER	Imported K3s	v1.24.9+k3s2	20 cores	78 GiB	65/110

Figure 1.

2. Once Active elect the cluster name and go to **Apps > Charts** and install the **GetVisibility Essentials** and **GetVisibility Monitoring Helm** charts:



GetVisibility Docker Image cache
A Helm chart for GetVisibility Kube auto fledged
Linux only

GetVisibility Docker Image Puller
A Helm chart for GetVisibility Kube auto puller
Linux only

GetVisibility Essentials
A Helm chart for GetVisibility Essential Services (Consul, Postgresql, Kafka, ElasticSearch and MinIO)
Linux only

GetVisibility Gatekeeper
A Helm chart for GetVisibility to enforce K8s policies
Linux only

GetVisibility Kafka Console
A Helm chart for Kafka-Console (only accessible in dev environment)
Linux only

GetVisibility Kafka UI
A Helm chart for Kafka-UI (only accessible in dev environment)
Linux only

GetVisibility Monitoring
Collects several related Helm charts, Grafana dashboards, and Prometheus rules combined with documentation and scripts to provide easy to operat...
Linux only

GetVisibility Private Registry
A Helm chart for GetVisibility Private Registry
Linux only

gv-model-deployer
GetVisibility Models
Linux only

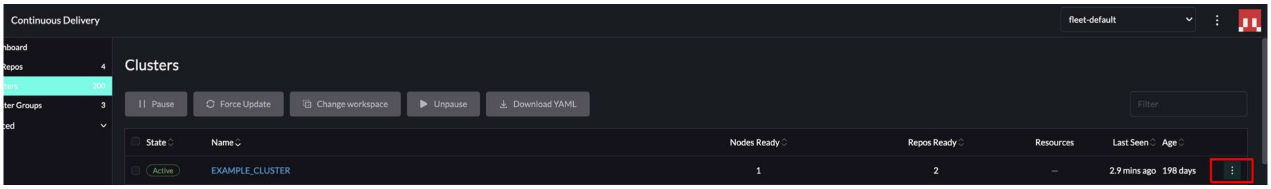
gv-models-csi
GetVisibility Models CSI mounter
Linux only

gv-platform
GetVisibility Platform
Linux only

Figure 2.

Use default values for both installations

3. Go to the global (burger) menu **Continuous Delivery > Clusters** and click on **Edit config** (three dots) for the cluster you are using:



State	Name	Nodes Ready	Repos Ready	Resources	Last Seen	Age
Active	EXAMPLE_CLUSTER	1	2	–	2.9 mins ago	198 days

Figure 3.

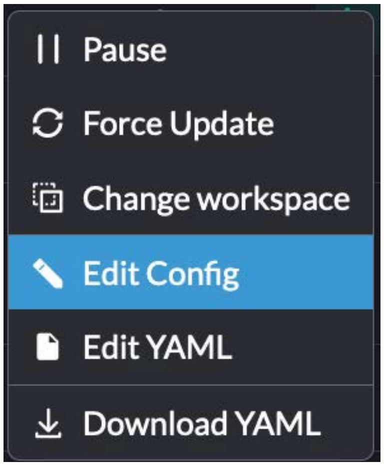
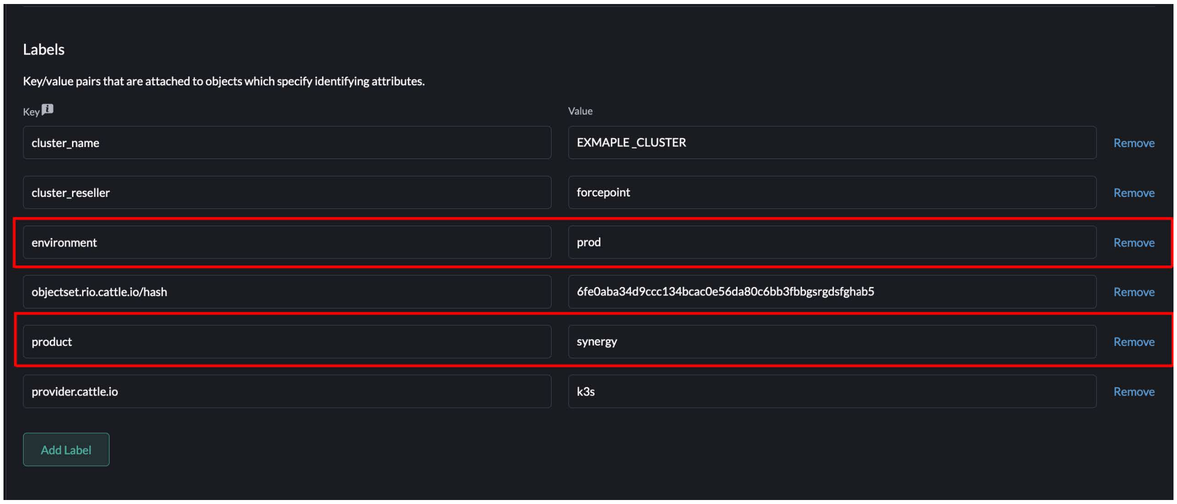


Figure 4.

4. Add 2 labels **product=synergy environment=prod** and press **Save**.



Labels

Key/value pairs that are attached to objects which specify identifying attributes.

Key	Value	
cluster_name	EXMAPLE _CLUSTER	Remove
cluster_reseller	forcepoint	Remove
environment	prod	Remove
objectset.rio.cattle.io/hash	6fe0aba34d9ccc134bcac0e56da80c6bb3fbbgsrgdsfghab5	Remove
product	synergy	Remove
provider.cattle.io	k3s	Remove

Figure 5.

The cluster is now set up and you can move onto user configuration.

Keycloak

Keycloak is an open-source product that allows Single Sign-On (SSO) and enables Identity and Access Management integration to allow for a quick, safe, and secure integration of authentication within modern applications.

When a cluster is generated via the Getvisibility reseller dashboard, it creates a Keycloak instance within the cluster for managing authentication.

When this cluster is created, a default Keycloak Realm configuration is loaded, and only a few installation steps are required.

This document describes the remaining installation steps required to complete the Keycloak installation setup.

Below are the steps involved in configuring Keycloak, and you may choose to skip the Optional steps based on your preferences:

Logging into Keycloak Admin Panel

The Keycloak admin URL will consist of the following components:

- The domain that has been configured for your reseller to access the application (E.g. my-dashboard.com or 10.10.121.127)
- The service path (E.g. auth for Keycloak)
- The keycloak admin path:

  ```
  /admin/master/console
  ```

An example of the above might look something like this:

https://my-dashboard.com/auth/admin/master/console

Once you have entered the correct address for your cluster Keycloak instance following the above guidelines, you should be able to log in to the Keycloak admin dashboard using the following details:

Username: admin

Password: admin

The access protocol should always be https.

The domain in the example above (e.g. my-dashboard.com) might not be applicable if a domain is not configured, in which case you would need to use the server IP address (e.g. 10.10.121.127).

Once logged into the portal, there are a few steps to complete to configure Keycloak.

Completing the Realm Configuration
In Keycloak, a **Realm** is a top-level authentication domain that contains an isolated authentication configuration.

A good way to imagine this is that each Keycloak Realm might represent a different environment.

We need to have a Realm for managing our cluster authentication, please follow the steps below to do this:

1. Make sure that the gv realm is selected in the top left, not master.

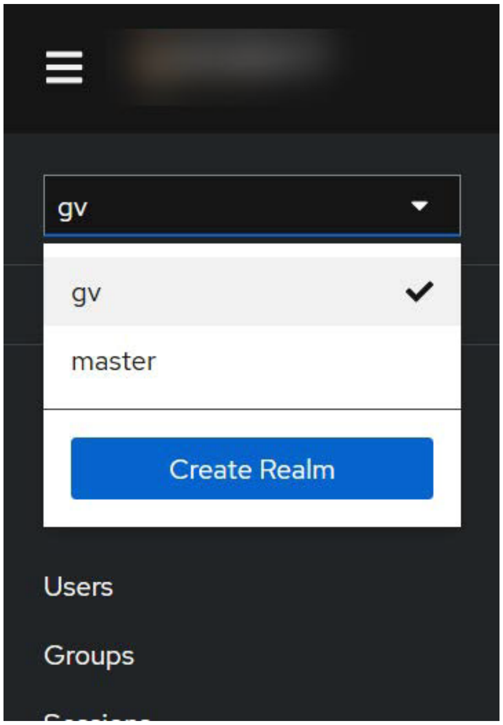


Figure 6.

2. Click on the left-side menu item **Realm settings**.

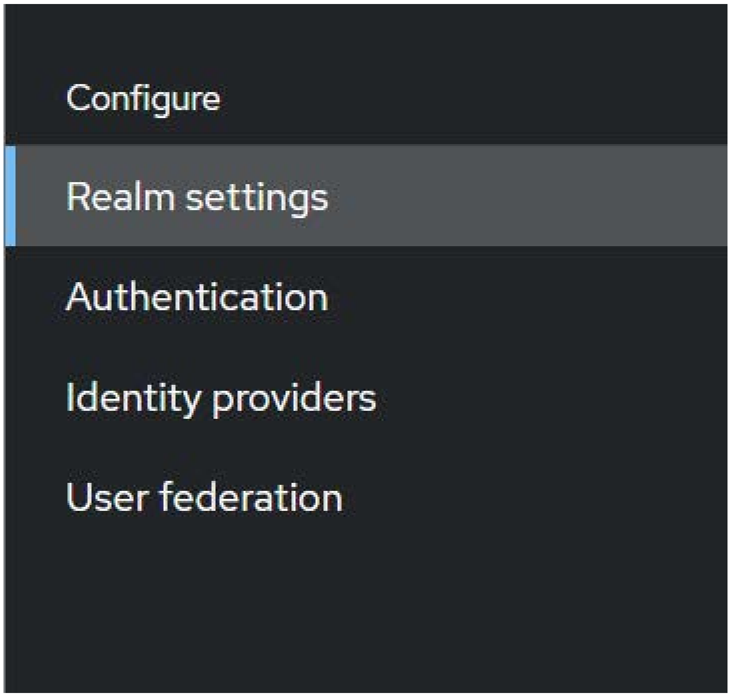
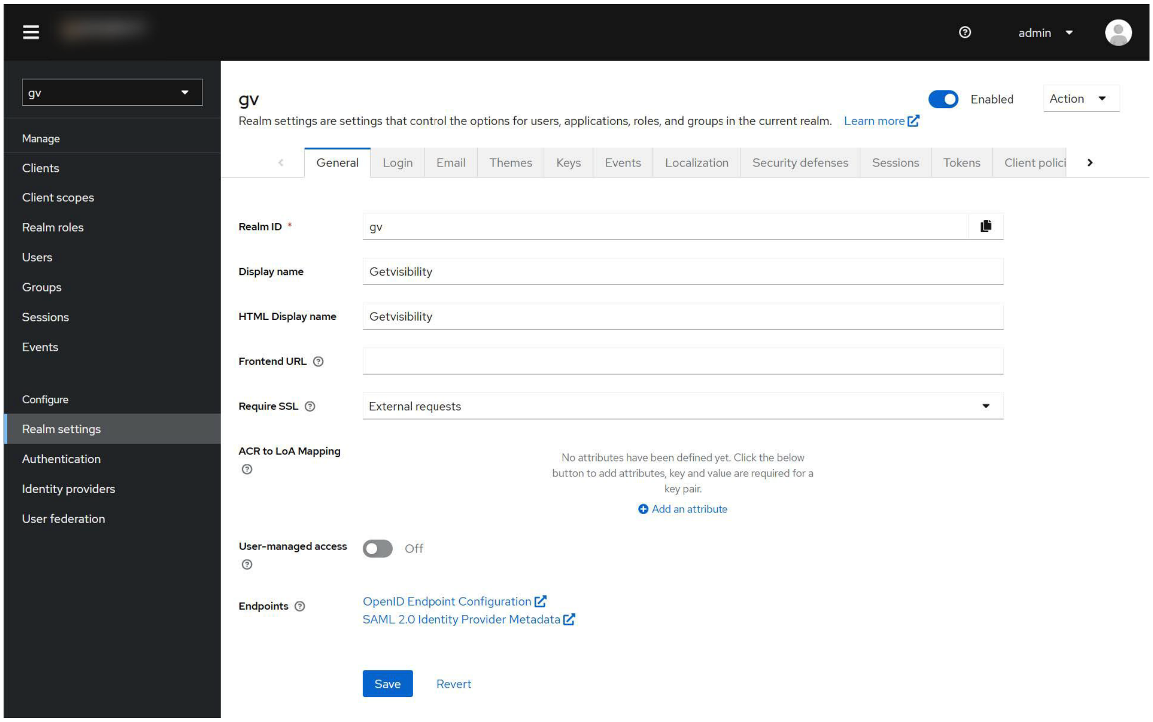


Figure 7.

3. This will load the **Gv Realm Settings** → **General** tab, enter your desired user-friendly **reseller** name into both the **Display name** and **HTML Display name** fields.



gv

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. Learn more

Realm ID * gv

Display name Getvisibility

HTML Display name Getvisibility

Frontend URL

Require SSL External requests

ACR to LoA Mapping

No attributes have been defined yet. Click the below button to add attributes, key and value are required for a key pair.

User-managed access Off

Endpoints OpenID Endpoint Configuration
SAML 2.0 Identity Provider Metadata

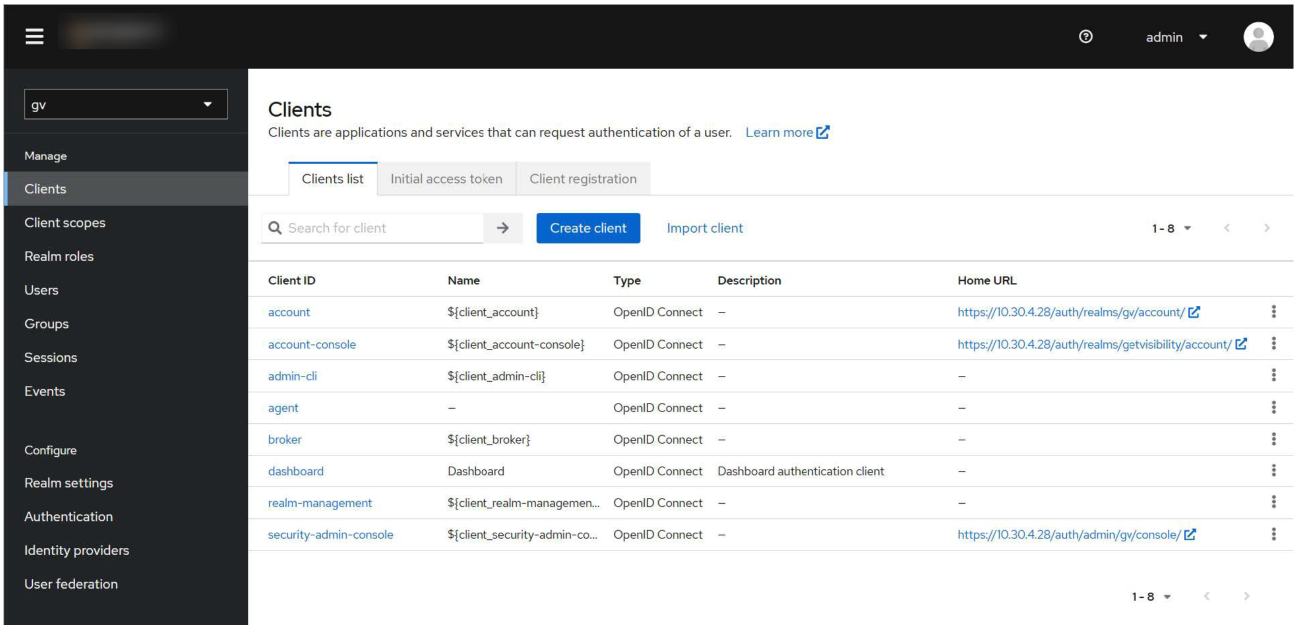
Figure 8.

4. Click the **Save** button to commit these changes to the Realm Settings.

⚠ Do not change the content of Realm ID field, it must be gv.

Completing the Dashboard Client Configuration

1. Click on the **Clients** menu item on the left-side menu, this should load a list of authentication clients.



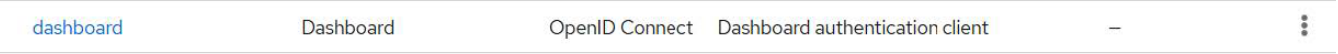
Clients

Clients are applications and services that can request authentication of a user. Learn more

Client ID	Name	Type	Description	Home URL
account	${client_account}	OpenID Connect	–	https://10.30.4.28/auth/realms/gv/account/
account-console	${client_account-console}	OpenID Connect	–	https://10.30.4.28/auth/realms/getvisibility/account/
admin-cli	${client_admin-cli}	OpenID Connect	–	–
agent	–	OpenID Connect	–	–
broker	${client_broker}	OpenID Connect	–	–
dashboard	Dashboard	OpenID Connect	Dashboard authentication client	–
realm-management	${client_realm-managemen...	OpenID Connect	–	–
security-admin-console	${client_security-admin-co...	OpenID Connect	–	https://10.30.4.28/auth/admin/gv/console/

Figure 9.

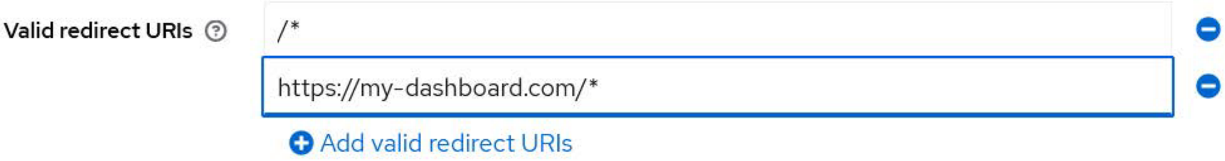
2. Click on the name link of the item labelled **dashboard** to navigate to its client configuration page.



dashboard	Dashboard	OpenID Connect	Dashboard authentication client	–

Figure 10.

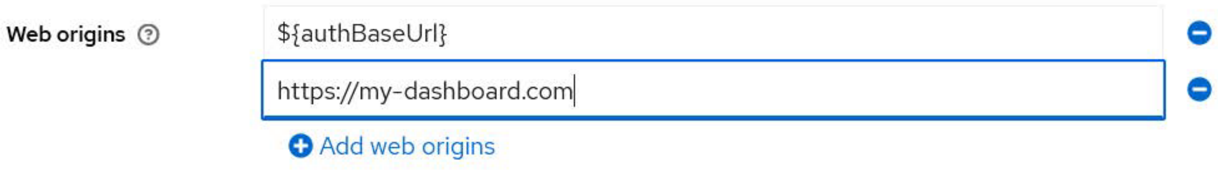
3. Update the **Valid Redirect URIs** to include the **URL** you have configured for the **Dashboard UI**. This will allow Keycloak to redirect back to your **Dashboard UI** after authenticating.



Valid redirect URIs: /*
https://my-dashboard.com/*

Figure 11.

4. Update the **Web Origins** to include the URL you have configured for the **Dashboard UI**. This will allow CORS endpoint calls to Keycloak from the Dashboard UI.



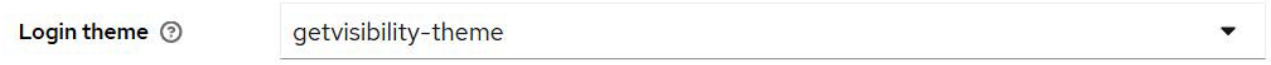
Web origins ⓘ

${authBaseUrl}

https://my-dashboard.com

Figure 12.

5. Open the dropdown for **Login Theme** and select the theme created for your reseller (E.g. **my-reseller-theme**).

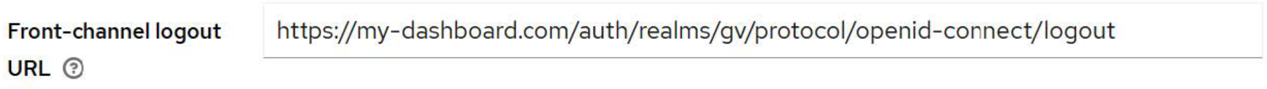


Login theme ⓘ getvisibility-theme ▼

Figure 13.

6. Clear the Front-channel logout URL field's content. This way, instead of the "you are getting logged out" screen, you'll get straight to the login page upon logout.
   Alternatively, you can enter the Front-channel logout URL in the following format:

   https://my-dashboard.com/auth/realms/gv/protocol/openid-connect/logout.



Front-channel logout URL ⓘ https://my-dashboard.com/auth/realms/gv/protocol/openid-connect/logout

Figure 14.

7. Click the **Save** button at the bottom of the screen.

(Required for FDC/Enterprise) Setting Up a Default Agent User

This step is important and required for the agent to work correctly. This user is only used internally by agents on endpoints to authenticate with the server. This user cannot be used to log in to the dashboard. For dashboard login, you must create your user in the gv realm.

1. Make sure it's still the **gv realm** selected in the top left, not master.

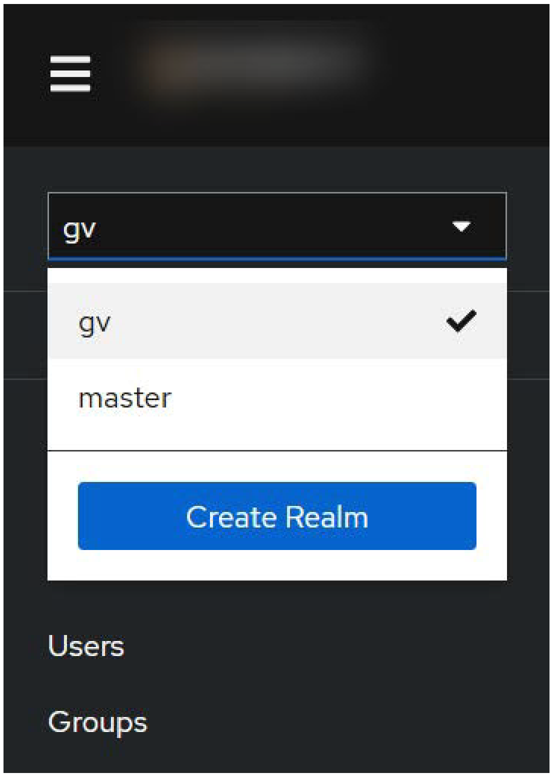


Figure 15.

2. Click on the **Users** menu item on the left-side menu, this should load the (empty) **Users** list.

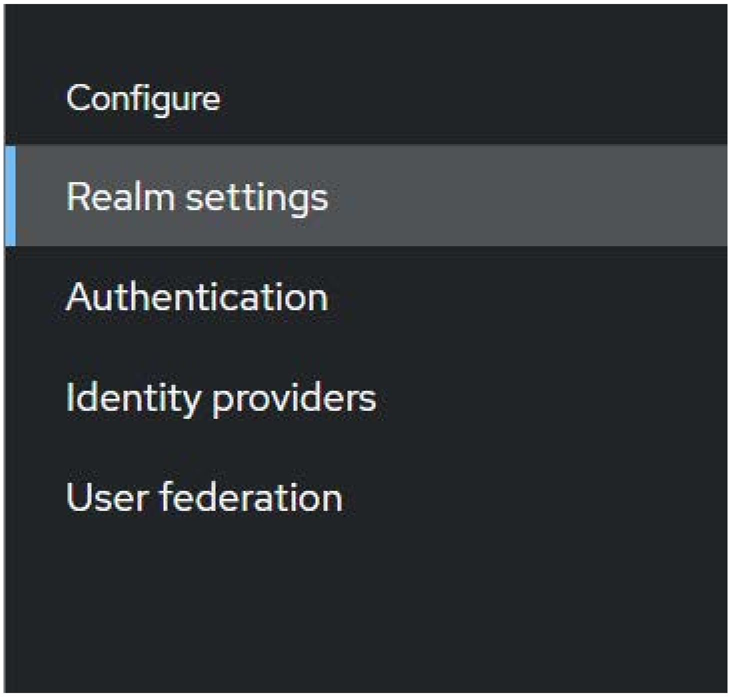
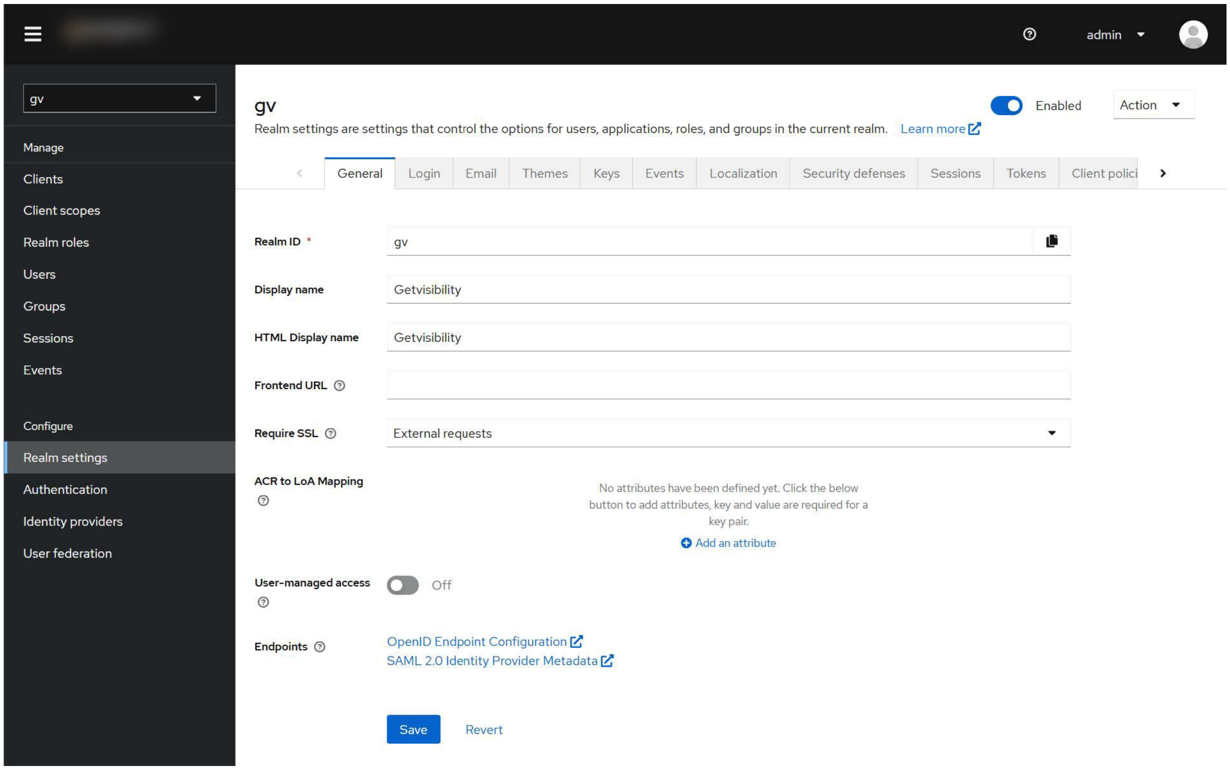


Figure 16.

3. Click the **Add user** button at the top to open the **Add user** screen.



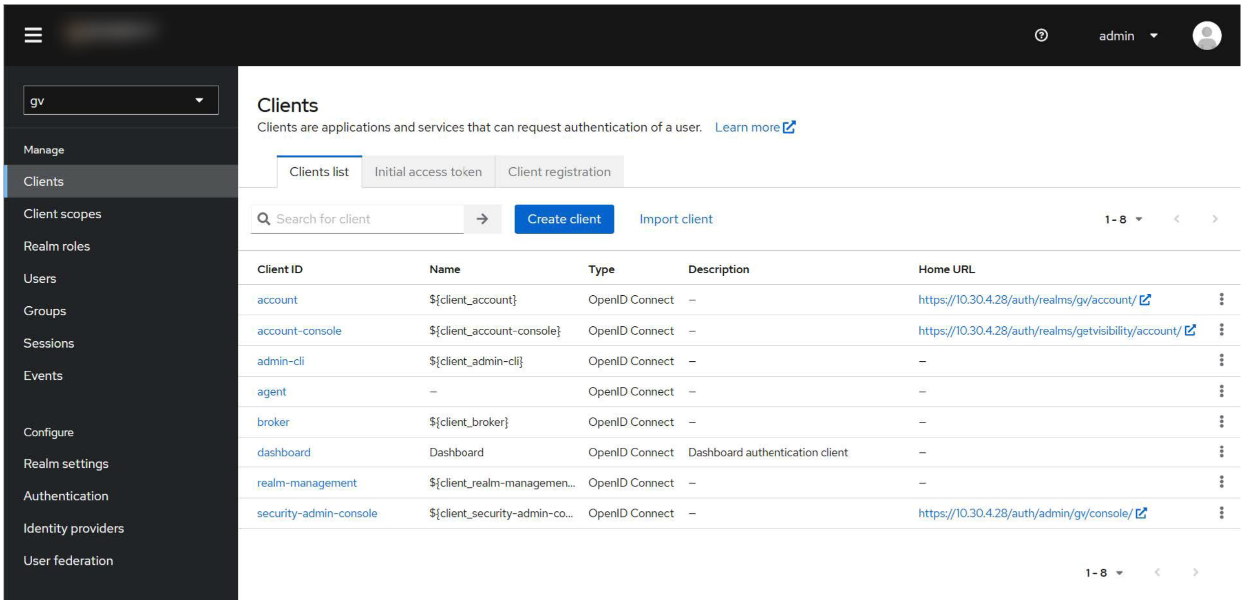
gv

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. Learn more

Realm ID *	gv
Display name	Getvisibility
HTML Display name	Getvisibility
Frontend URL	
Require SSL	External requests
ACR to LoA Mapping	No attributes have been defined yet. Click the below button to add attributes, key and value are required for a key pair.
User-managed access	Off
Endpoints	OpenID Endpoint Configuration SAML 2.0 Identity Provider Metadata

Figure 17.

4. It's only necessary to complete two fields on this form; The **Username** field should contain **agent**, and the **Email** field should contain **agent@gv.com.**



Clients

Clients are applications and services that can request authentication of a user. Learn more

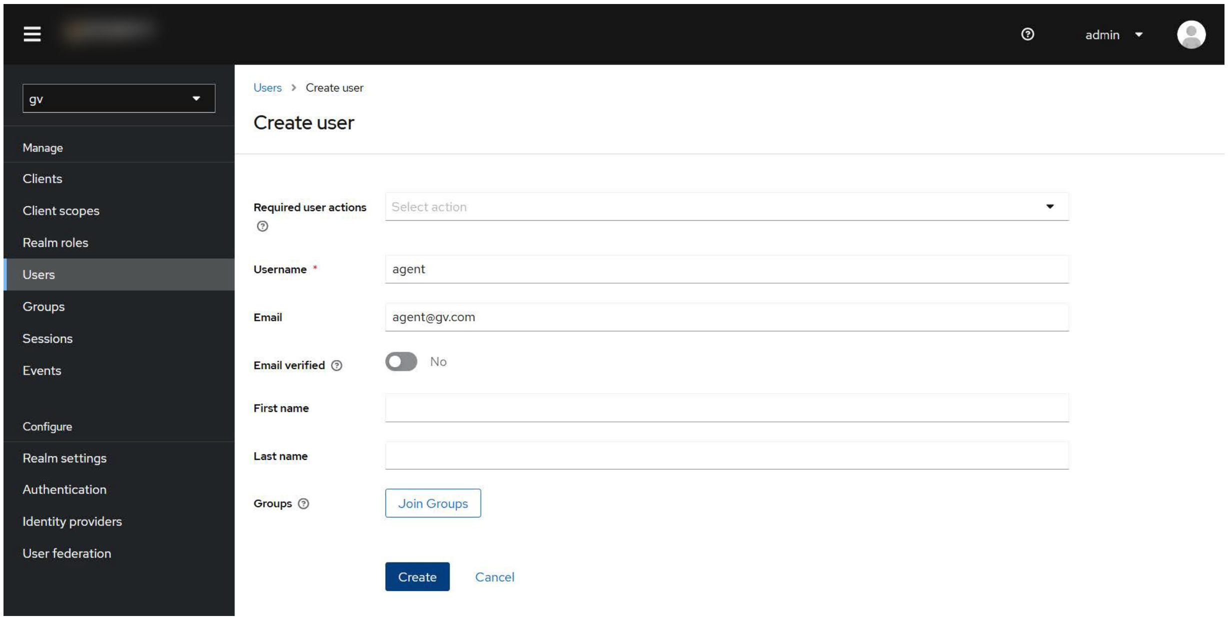
Client ID	Name	Type	Description	Home URL
account	${client_account}	OpenID Connect	–	https://10.30.4.28/auth/realms/gv/account/
account-console	${client_account-console}	OpenID Connect	–	https://10.30.4.28/auth/realms/getvisibility/account/
admin-cli	${client_admin-cli}	OpenID Connect	–	–
agent	–	OpenID Connect	–	–
broker	${client_broker}	OpenID Connect	–	–
dashboard	Dashboard	OpenID Connect	Dashboard authentication client	–
realm-management	${client_realm-managemen...	OpenID Connect	–	–
security-admin-console	${client_security-admin-co...	OpenID Connect	–	https://10.30.4.28/auth/admin/gv/console/

Figure 18.

5. Click the **Create** button at the bottom of the screen.

(Optional) Completing the Agent Client Configuration

1. Click on the Clients menu item on the left-side menu, this should load a list of authentication clients.

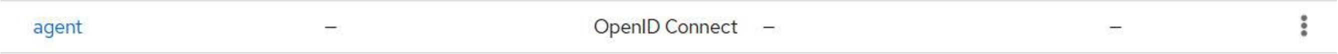


Create user

Required user actions	Select action
Username *	agent
Email	agent@gv.com
Email verified	No
First name	
Last name	
Groups	Join Groups

Figure 19.

2. Click on the name link of the item labelled **agent** to navigate to its client configuration page.

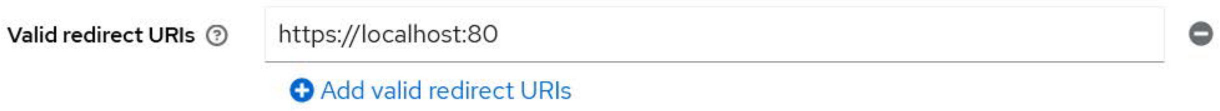


agent	–	OpenID Connect	–	–

Figure 20.

3. Update the **Valid Redirect URIs** value (default is **https://localhost:80**) to a secure address you know is not vulnerable or exposed.

   This is a required field and requires at least one value, so while we have set it to a temporary value, it's encouraged to change this to something internal.



Valid redirect URIs: https://localhost:80

Figure 21.

4. Click the **Save** button at the bottom of the screen.

Creating a User to Access the Getvisibility Dashboard

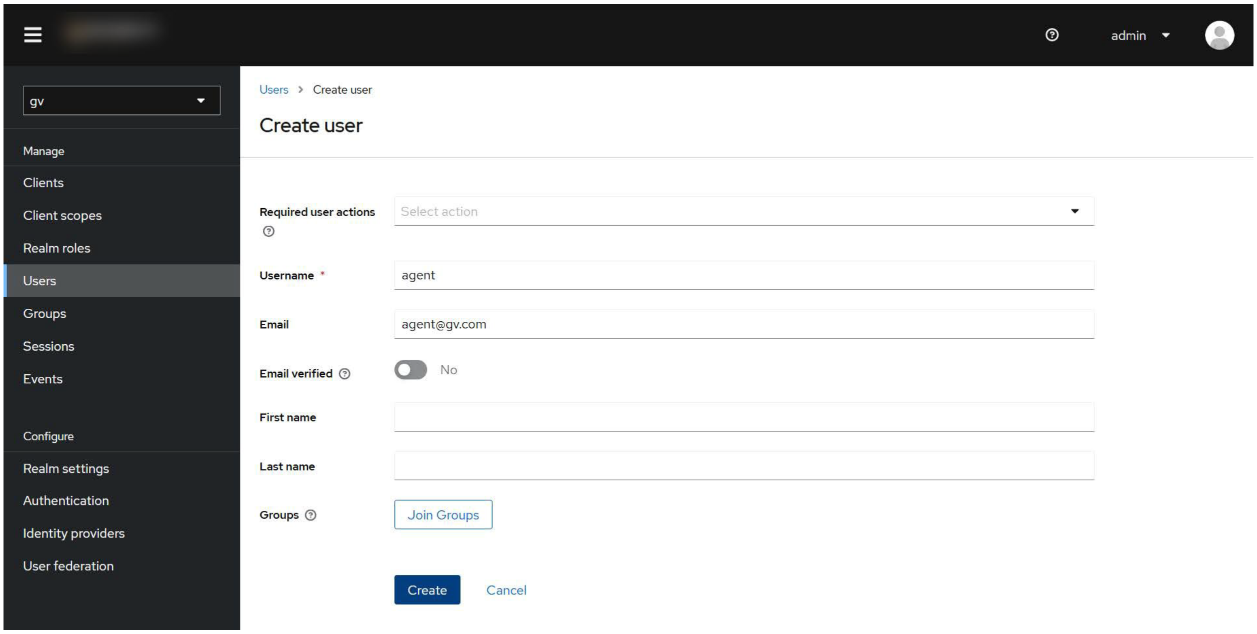
⚠ By default, there are no users in the gv realm, meaning that nobody can access the dashboard to view agent activity, use analytics, run scans, or create reports.

⚠ Users must either be created manually as described below, or imported, e.g. via LDAP user federation.

ℹ Users created in the gv realm will have full administrative access to the GetVisibility web console.

RBAC implementation for granular management of dashboard user permissions is on our roadmap.

1. Make sure that it's still the gv realm selected in the top left, not master:



Required user actions: Select action

Username *: agent

Email: agent@gv.com

Email verified: No

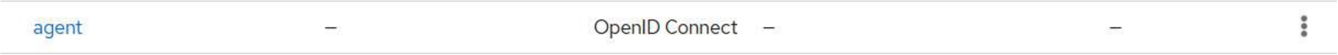
First name:

Last name:

Groups:

Figure 22.

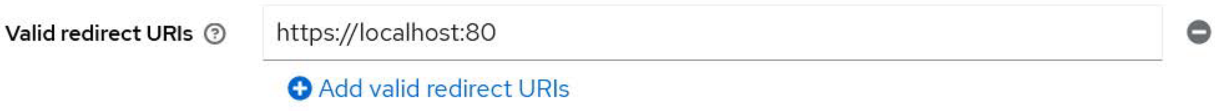
2. Click on the Users menu item on the left-side menu, this should load the (empty) **Users** list.



agent – OpenID Connect – –

Figure 23.

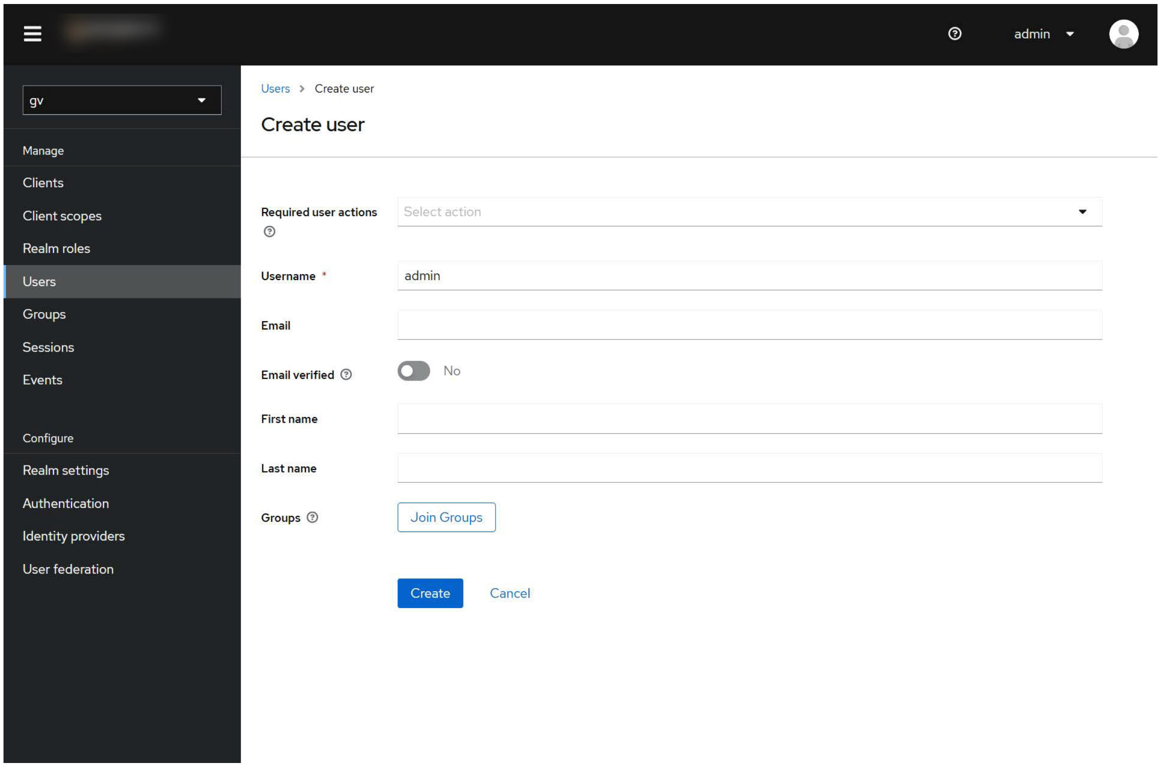
3. Click the **Add user** button at the top to open the **Add user** screen.



Valid redirect URIs: https://localhost:80

Figure 24.

4. There is only one mandatory field here; The **Username** field should contain your desired username, e.g. **admin**.



Create user

Required user actions: Select action

Username *: admin

Email:

Email verified: No

First name:

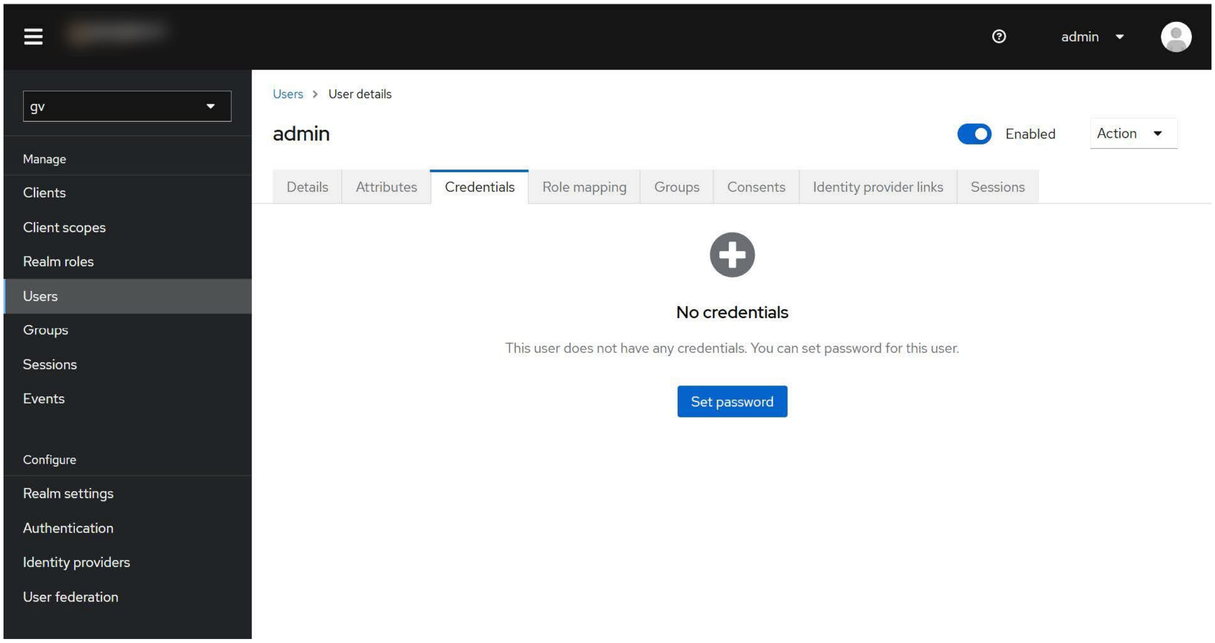
Last name:

Groups: Join Groups

Figure 25.

5. Click **Create**. You will automatically get redirected to the **User Details** page of the user you just created.

6. Here, click **Set password**.



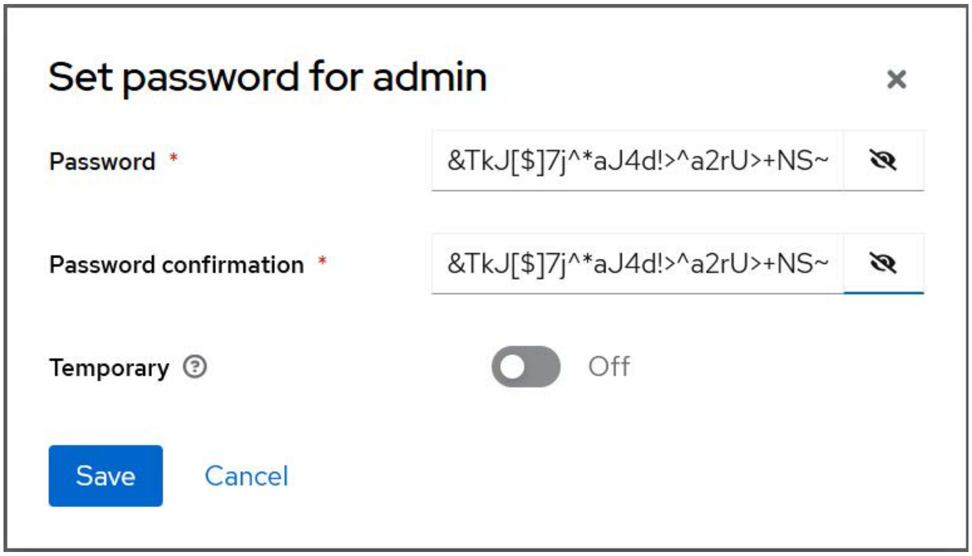
admin

No credentials

This user does not have any credentials. You can set password for this user.

Figure 26.

Next, choose a strong password for the user. Leave the “Temporary” option on if you want the user to change their password on the first login.



Set password for admin

Password * &TkJ[$]7j^*aJ4d!>^a2rU>+NS~

Password confirmation * &TkJ[$]7j^*aJ4d!>^a2rU>+NS~

Temporary Off

Figure 27.

7. Click **Save**.
8. Navigate to the /ui endpoint of the IP of the server or the domain if you configured any. E.g. **https://my-dashboard.com/ui or https://10.10.121.127/ui**

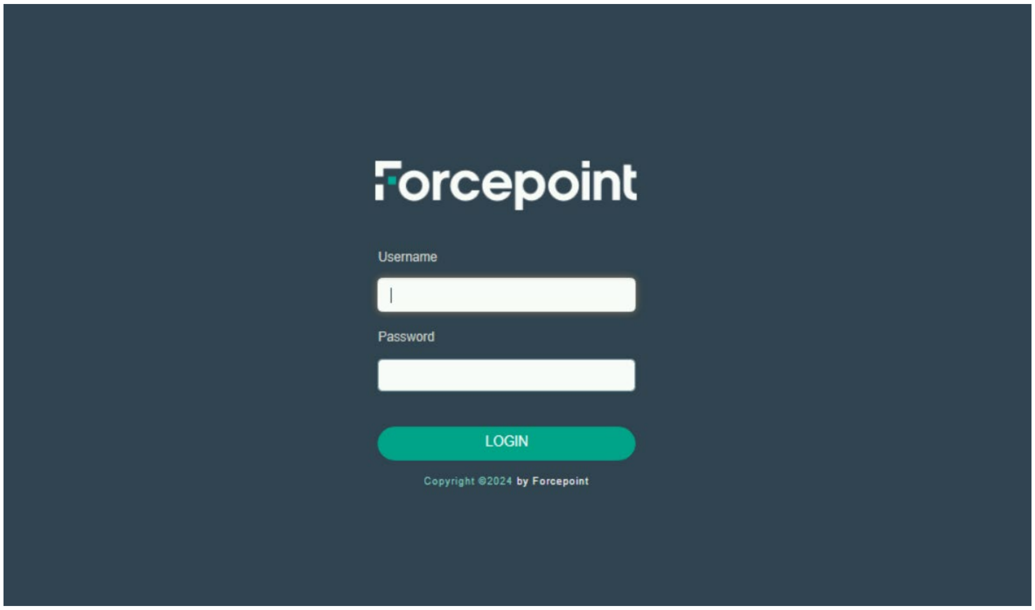


Figure 28.

Confirm that the credentials are working as expected.

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[Forcepoint Data Security Posture Management Powered by GetVisibility FDC Server Installation Guide] [Status]23 Jul. 24