



# **Administrator Guide**

Version 426151b

---

# Table of Contents

---

<b>What's New?</b>	<b>3</b>	Inviting Administrators	18
<b>Common Terms</b>	<b>4</b>	Accepting Network Invites	19
<b>Super Administrator</b>	<b>4</b>	Bot Management	20
Administrator Login	5	Network Profile	22
Super Administrator Settings	6	SSO Configuration	23
Creating a Network Administrator	8	Event Logging	24
Manage the Room Bot	9	Client Configuration	25
Crash Reports	10	Wickr Open Access	29
Registration and Administrator Lockout	10	Default Rooms	30
Manage Global Federation	11	API Access	31
Generate API Access Tokens	13		
<b>Network Administrator</b>	<b>14</b>	<b>Security Groups</b>	<b>32</b>
Dashboard	14	General	33
Account Settings	15	Messaging	34
Team Directory	16	Federation	39

# What's New?

---

## 426151b

**Optional TLS Cert Pinning** – clients can now be configured to use standard system certificate validation for TLS instead of pinning to specific certificates.

### **Stability and Bug Fixes**

# Common Terms

---

**Super Administrator:** Can create and manage network administrators

**Network:** A group of users allowed to find and communicate with each other by default

**Network Administrator:** Can create new networks and provision users within a network

**Security Group:** Specific settings for users within a network

**Expiration:** The maximum amount of time a message will live across all devices

**Verification:** Additional security for users to verify their contact is who they should be

**Federation:** Allows communication between different networks

**Global Federation:** Allows communication outside the local Enterprise deployment

**Direct Message:** A private conversation between two users. Each user manages their expiration and BOR settings.

**Room:** A group of users with settings managed by Moderators. Up to 500 users in a room.

**Group:** A group of users who each manage their own message settings.

**Wickr Open Access:** An additional method of network traffic obfuscation

**User Presence:** Users can view other users' app idle time

**Location:** Users can share their location via link or map

**Live Location:** Users can share their location over a set period of time. (Android and iOS only.)

**Link Previews:** Shows a header and image of the link being shared as a preview.

## Super Administrator

---

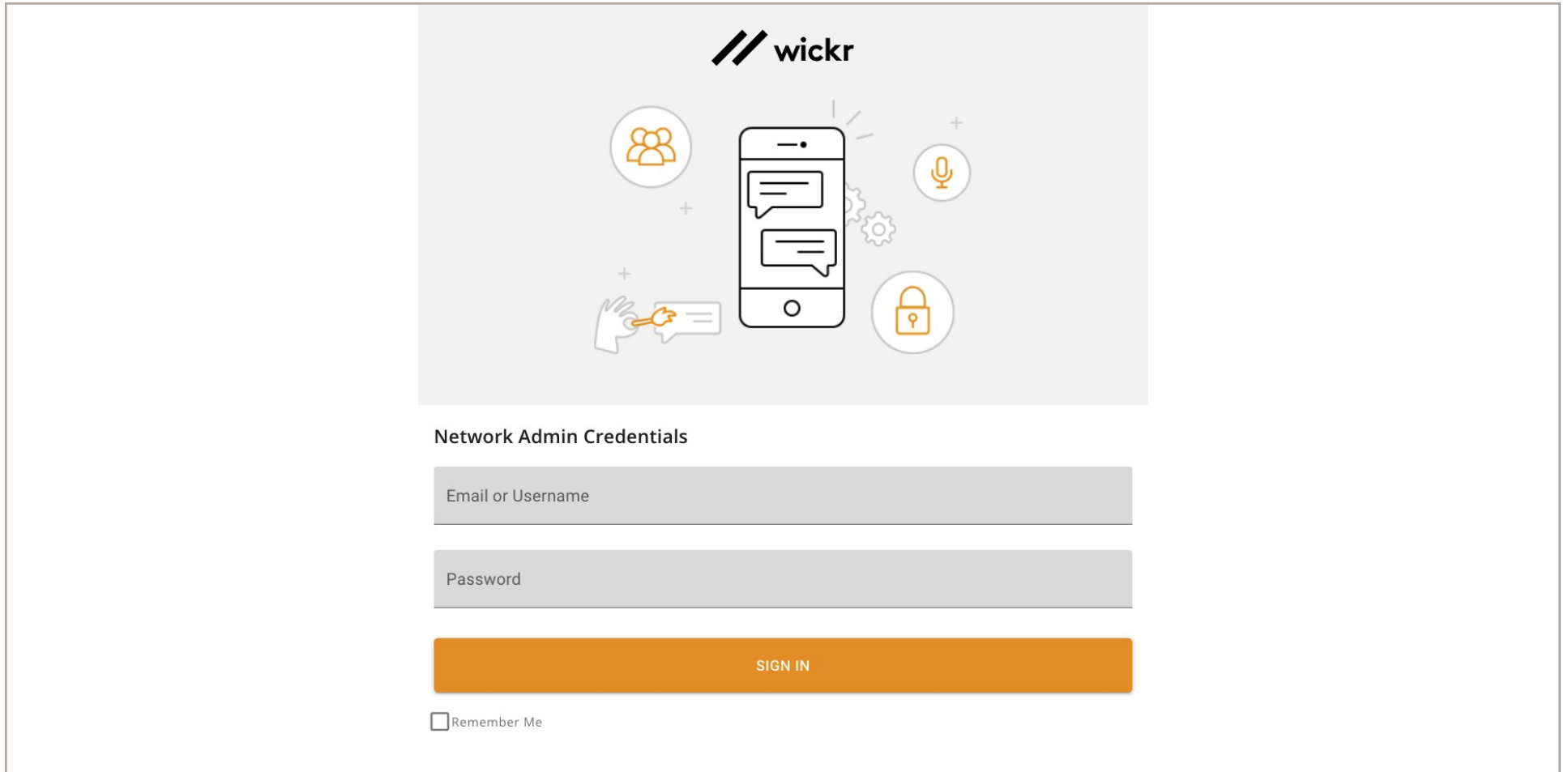
The first step in getting started with Wickr Enterprise is signing in as the Super Administrator. The super administrator can provision, update, and delete network administrators.

### IMPORTANT

*Super Administrator and Network Administrator usernames are separate from normal users. This means Administrators cannot login to the Wickr apps and normal users cannot login to the Admin Panel.*

# Administrator Login

Enter your username and password and click LOG IN to enter the Super Administrator console as shown below.




The image shows the Wickr Administrator Login interface. At the top, the Wickr logo is displayed. Below the logo is a central graphic featuring a smartphone with a speech bubble, surrounded by icons for users, a microphone, a hand holding a key, and a padlock. Below this graphic is the section titled "Network Admin Credentials". It contains two input fields: "Email or Username" and "Password". Below the password field is a prominent orange "SIGN IN" button. At the bottom left of the form is a checkbox labeled "Remember Me".

## IMPORTANT

*Only one active session per logged in Administrator is allowed.  
If the same Administrator logs in again from a different browser, it will log out the other session.*

# Super Administrator Settings

Once logged into the Super Administration panel you'll be forced to change the default password. You can also enable 2 Factor Authentication using your preferred authenticator. We recommend Google Authenticator, but any OTP Auth software will work.



Wickr Admin  
admin

- Super Admin
- Manage Room Bot
- Crash Report
- Lockout
- Global Federation
- API Access Tokens
- Legacy Dashboard

5.72.0  
**SIGN OUT**

### My Account

#### Personal Information

#### Administrator Password

This is your password for the Wickr network dashboard. Please note that it is distinct from the password used to access your Wickr app.

**CHANGE**

#### Two Factor Authentication

OFF

## IMPORTANT

*It is not possible to reset the Super Administrator account if the authentication method for 2FA is lost.*

The available functions of the Super Administrator are:

- To manage Network Administrators
- Enabling or Disabling the Room Bot
- To unlock Network Administrators who have entered their password correctly
- To manage Global Federation
- To manage API keys with access to the every Network in the Enterprise deploy

The screenshot displays the Wickr Admin interface for a Super Administrator. The sidebar on the left contains the Wickr logo, the user's name 'Wickr Admin admin', and a list of navigation items: Super Admin, Manage Room Bot, Crash Report, Lockout, Global Federation, API Access Tokens, and Legacy Dashboard. At the bottom of the sidebar, the version '5.72.0' and a 'SIGN OUT' button are visible. The main content area is titled 'Admins' and features a 'CREATE NEW ADMIN' button and a search bar. Below this is a table with columns for Username, First Name, Last Name, and Network Membership. A single row is shown for 'network\_admin' with a dropdown menu icon. The dropdown menu is open, showing 'Edit' and 'Delete' options, which are highlighted with an orange border.

Username	First Name	Last Name	Network Membership
<input type="checkbox"/> network_admin	Network	Administrator	network_admin's netw

# Creating a Network Administrator

Once logged into the Super Administration panel you can create network administrators. Network administrators will be able to configure their own networks, security groups, and manage end users.

- To create a network administrator, fill in their username and password. First and last name are optional.
- Network administrators can be added to an existing network using the network drop down or be assigned to a new network.
- Network administrators' passwords can be updated at any time from this screen.
- Network administrators can be deleted from this screen.

We recommend at least two administrators per network. Having multiple administrators ensures that you have maximum coverage in the case of any emergencies.

The screenshot shows the 'New Admin' form in the Wickr Enterprise Administrator interface. The form is centered and contains the following sections:

- Admin Information**
  - First Name: [Empty text input]
  - Network: [Dropdown menu with 'Network' selected]
  - Last Name: [Empty text input]
  - Administrator: [Empty text input]
- Account Information**
  - Username: [Text input with 'network\_admin' entered]
  - Password: [Password input with '.....' entered]
  - Repeat Password: [Password input with '.....' entered]
- Create new network: [Dropdown menu with 'Create new network' selected]

At the bottom of the form are two buttons: 'CANCEL' and 'CREATE'.

The background shows a sidebar with navigation options: Manage Room Bot, Crash Report, Lockout, Global Federation, API Access Tokens, and Legacy Dashboard. The version number 5.72.0 and a 'SIGN OUT' button are also visible. On the right, a 'Network Membership' section is partially visible.










# Manage the Room Bot

The Room Bot allows Network Administrators to deploy pre-created rooms managed by this bot. The bot will add all users in a particular Security Group or Network to a room and automatically re-add users if they attempt to leave.

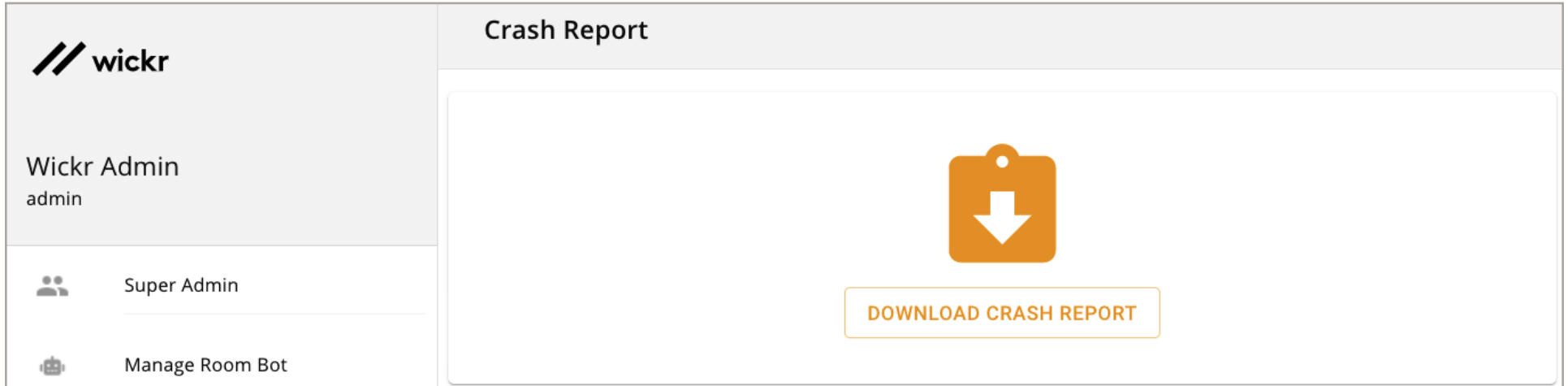
Multiple rooms can be created for any group.

This bot is off by default and can be disabled anytime. If disabled after Network Administrators have created rooms, any active rooms will still exist however they will not be able to be managed and will always have the same members.

  Wickr Admin admin	<h2>Manage Room Bot</h2>
<ul style="list-style-type: none"><li> Super Admin</li><li> <b>Manage Room Bot</b></li><li> Crash Report</li><li> Lockout</li><li> Global Federation</li><li> API Access Tokens</li></ul>	<p>The default room bot is currently Active</p> <p><b>DISABLE ROOM BOT</b></p>

# Crash Reports

Super Administrators can also generate Crash Reports in the case of any failures. Please provide this to Wickr in the event of any failures, however it should be noted that these files and more are available server side and via Replicated.




**wickr**

Wickr Admin  
admin

Super Admin

Manage Room Bot

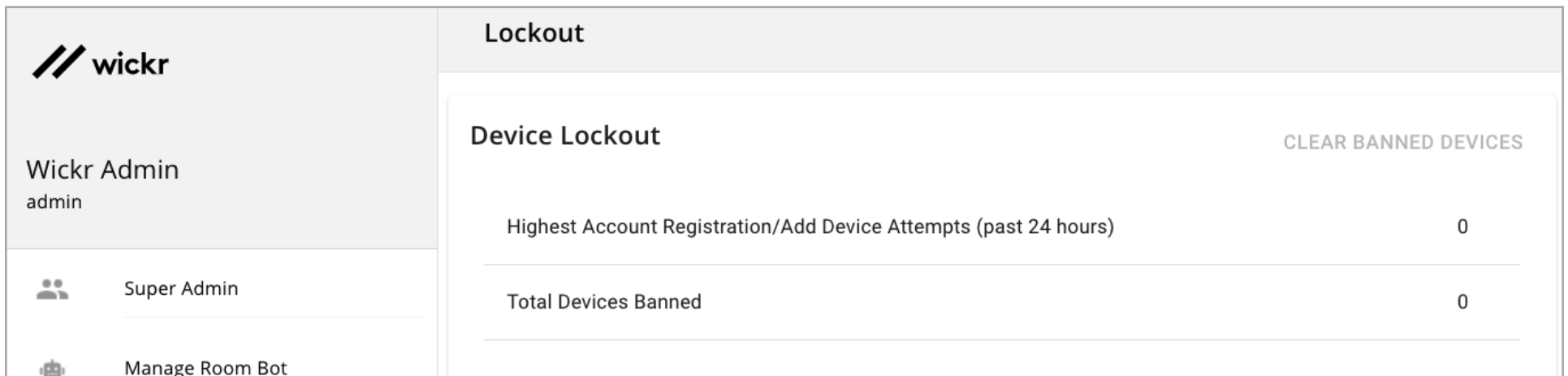
## Crash Report



DOWNLOAD CRASH REPORT

# Registration and Administrator Lockout

Super Administrators are also able to unlock Network administrators accounts if they become locked after unsuccessful login attempts via the Lockout tab. A status showing the total number of devices that are locked out as well as a count of the number of registration attempts can be seen on this page.



**wickr**

Wickr Admin  
admin

Super Admin

Manage Room Bot

## Lockout

### Device Lockout

CLEAR BANNED DEVICES

Highest Account Registration/Add Device Attempts (past 24 hours)	0
Total Devices Banned	0

# Manage Global Federation

Global Federation (GF) allows Wickr Enterprise to communicate with other Enterprise deployments as well as Wickr Me and Wickr Pro.

This access must be approved and enabled on both deploys for a successful connection, so it cannot be federated without mutual agreement of all parties.

For Wickr Me or Pro federation please contact Wickr Support to white list your deployment.

The Global Federation capability is explained in detail in the Global Federation: Setup and Configuration Guide.

The screenshot displays the Wickr Admin interface. On the left is a sidebar with the user 'Wickr Admin admin' and navigation options: Super Admin, Manage Room Bot, Crash Report, Lockout, Global Federation (highlighted), API Access Tokens, and Legacy Dashboard. At the bottom of the sidebar is a 'SIGN OUT' button with version '5.72.0'. The main content area is titled 'Global Federation' and contains the following sections:

- Global Federation**: A text block explaining that Wickr Global Federation allows users in the current infrastructure to communicate with other Wickr Enterprise infrastructures and Wickr Messenger. It states that to communicate with another Wickr Enterprise infrastructure, the user must provide their Federation Domain and API Key.
- Federation ID**: A section with the instruction 'Share your network credentials with the partner Wickr infrastructure to establish federation'. It contains two rows of input fields:
  - Domain**: A field containing '107 65' and a 'COPY' button.
  - API Key**: A field containing 'yfy+OhBrH NsaGVa//VA=' and a 'COPY' button.
- Wickr Messenger Federation**: A section with the instruction 'Select this option to enable federation with Wickr Me. Once this option is enabled, please contact Wickr support in order to complete enabling federation with Wickr Me.' It includes a toggle switch for 'Wickr Messenger Federation' which is currently turned off.
- Wickr Pro Federation**: A section with the instruction 'Select this option to enable federation with Wickr Pro. Once this option is enabled, please contact Wickr support in order to complete enabling federation with Wickr Pro.' It includes a toggle switch for 'Wickr Pro Federation' which is currently turned off.
- Federated Wickr Infrastructures**: A section with a '+ Add Infrastructure' button and the text 'Below is a list of Wickr Enterprise domains that are allowed to communicate with this'.

Global Federation requires domain names and a new username style to be used.

**Federated Wickr Infrastructures:** These are the **EXTERNAL** domains allowed to communicate with this deployment. The API key for that domain must be added with the domain name.

**Local Domains For Federation:** These are the **INTERNAL** domains used for usernames within this deployment. A DNS record or other identifying information is needed for other Enterprise deployments to connect successfully.

These local domains will be the only allowed domain names used when creating new users:

For example, if the domain “example.com” and “testing.com” were added here, the following users would be valid:

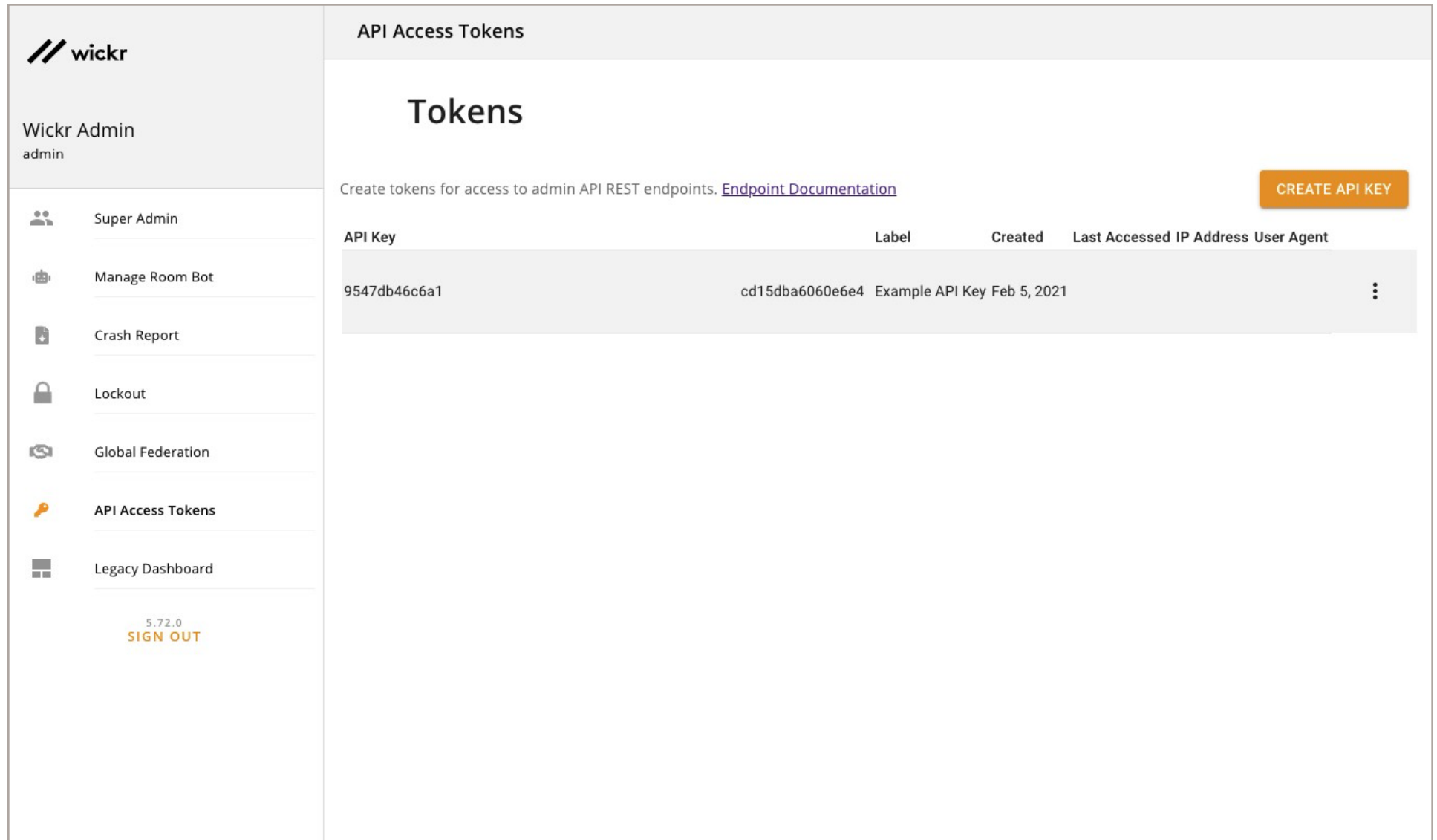
- **userone@example.com**
- **georgio@testing.com**

The screenshot displays the Wickr Enterprise Administrator interface. On the left is a sidebar with navigation options: 'API Access Tokens' (with a key icon) and 'Legacy Dashboard' (with a grid icon). Below these is the version '5.72.0' and a 'SIGN OUT' button. The main content area is titled 'Wickr Messenger Federation' and contains a toggle switch that is currently turned off. Below this is the 'Wickr Pro Federation' section, also with a turned-off toggle switch. The 'Federated Wickr Infrastructures' section includes a '+ Add Infrastructure' button and a table with columns for 'Domain' and 'API Key'. The 'Local Domains For Federation' section includes a '+ Add Domain' button and a table with a 'Domain' column.

# Generate API Access Tokens

Super Administrators can generate an API Token that has access to any network and security group within the Enterprise deployment.

Documentation for the API can be found within the deployment using the **Endpoint Documentation** link above the token list.



The screenshot displays the Wickr Admin interface for managing API Access Tokens. The sidebar on the left contains navigation links: Super Admin, Manage Room Bot, Crash Report, Lockout, Global Federation, API Access Tokens (highlighted), and Legacy Dashboard. At the bottom of the sidebar, the version 5.72.0 and a SIGN OUT button are visible.

The main content area is titled 'API Access Tokens' and 'Tokens'. It includes a 'CREATE API KEY' button and a table of existing tokens. The table has the following columns: API Key, Label, Created, Last Accessed, IP Address, and User Agent.

API Key	Label	Created	Last Accessed	IP Address	User Agent
9547db46c6a1	cd15dba6060e6e4 Example API Key	Feb 5, 2021			

# Network Administrator

## Dashboard

Once credentials have been made for a Network Administrator they can login using the same URL as the Super Administrator.

The administrator console is comprised of the [Dashboard](#), [User Settings](#), [Network Settings](#), and [FAQ](#). We will cover each section in detail in the next few pages.

The initial login screen is shown below.

**wickr**

Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User ▾
- Network Settings ▾
- FAQ
- Legacy Dashboard

5.72.0  
**SIGN OUT**

### Wickr Network Dashboard

0  
ACTIVE USERS

0  
PENDING USERS

#### Team Directory

Total Users: 1

Check the status of your employees and invite more.

**INVITE** **MANAGE**

#### Network Profile

Update name and icon of your network

Network Administrator

network\_admin

Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens
- FAQ

# Account Settings

Clicking the username will open the Personal Settings menu. You can change your first and last names, change your password, or enable 2 Factor Authentication here.

**My Account**

**Personal Information**

First Name  
Network

Last Name  
Administrator

**Administrator Password**

This is your password for the Wickr network dashboard. Please note that it is distinct from the password used to access your Wickr app.

**CHANGE**

**Two Factor Authentication**

OFF

Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
- Team Directory**
- Bot Management
- Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens
- FAQ

## Team Directory

When not using SSO, an Administrator can manually add users here. They can be made individually or by uploading a CSV file in the proper format. An example CSV can be downloaded to modify.

User statuses can be:

- **Pending:** The user has not registered.
- **Active:** The user has registered and is able to receive messages.
- **Suspended:** The user is unable to sign in to their account, but still active.
- **Restricted:** This notes that the user cannot use Global Federation or is strictly an Administrator.

If there is a requirement to restrict the types of devices your users can use with Wickr Enterprise we recommend using a Mobile Device Management (MDM) solution.

User types are:

- **User:** This user can login to the Wickr Enterprise apps.
- **Web Admin:** This user can only log into the Network Dashboard.

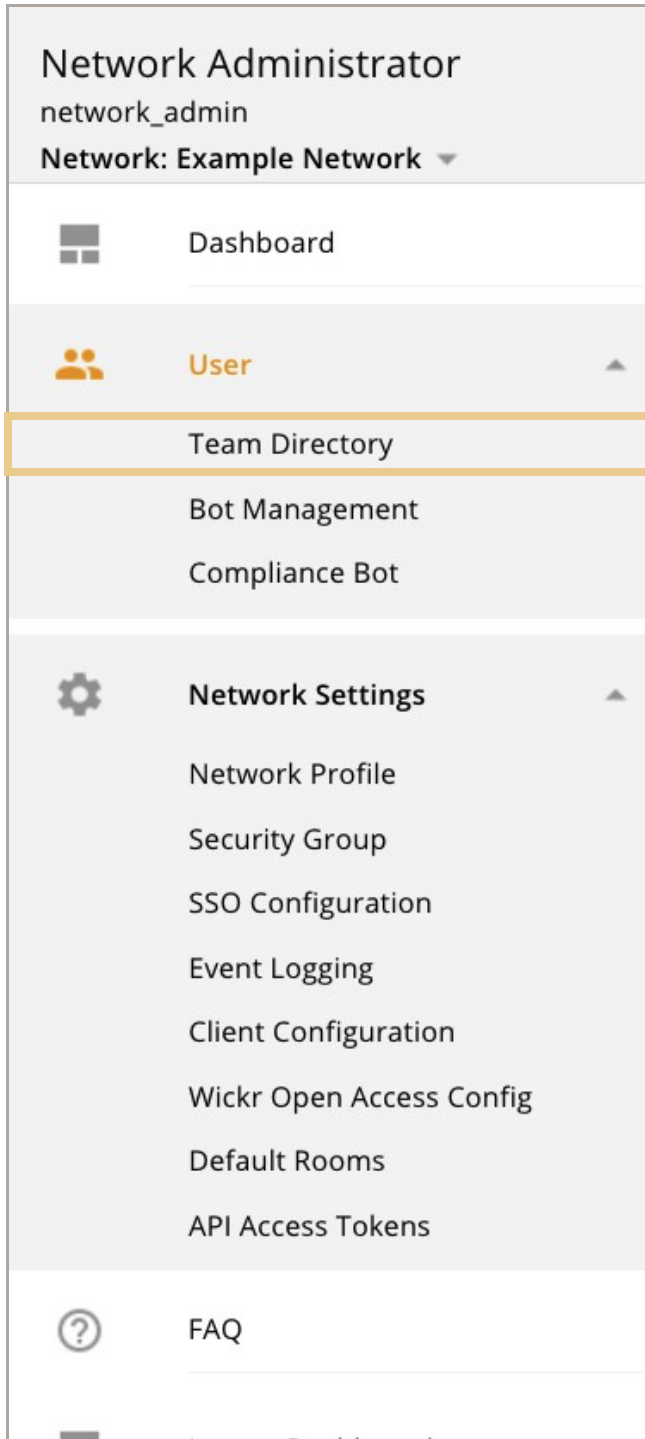
Team Directory 📄 +

### Users

[CREATE NEW USER](#)

	Email or Username ▲	First Name	Last Name	Type	Security Group	Status	
<input type="checkbox"/>	giorgio@testing.com	Giovanni	Giorgio	user	default	pending	⋮
<input type="checkbox"/>	network_admin			web admin		restricted	⋮
<input type="checkbox"/>	userone@example.com	Example	User	user	default	pending	⋮



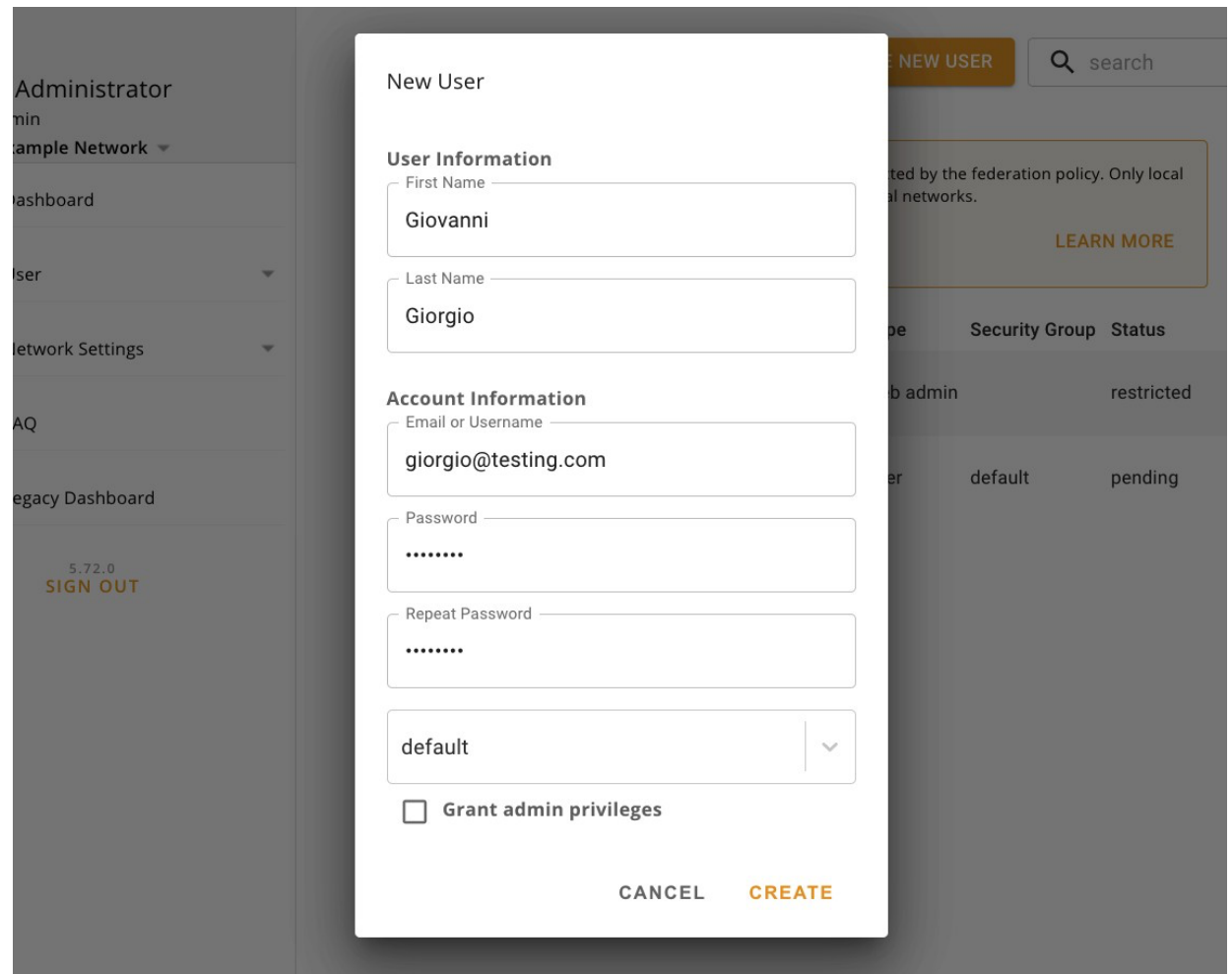


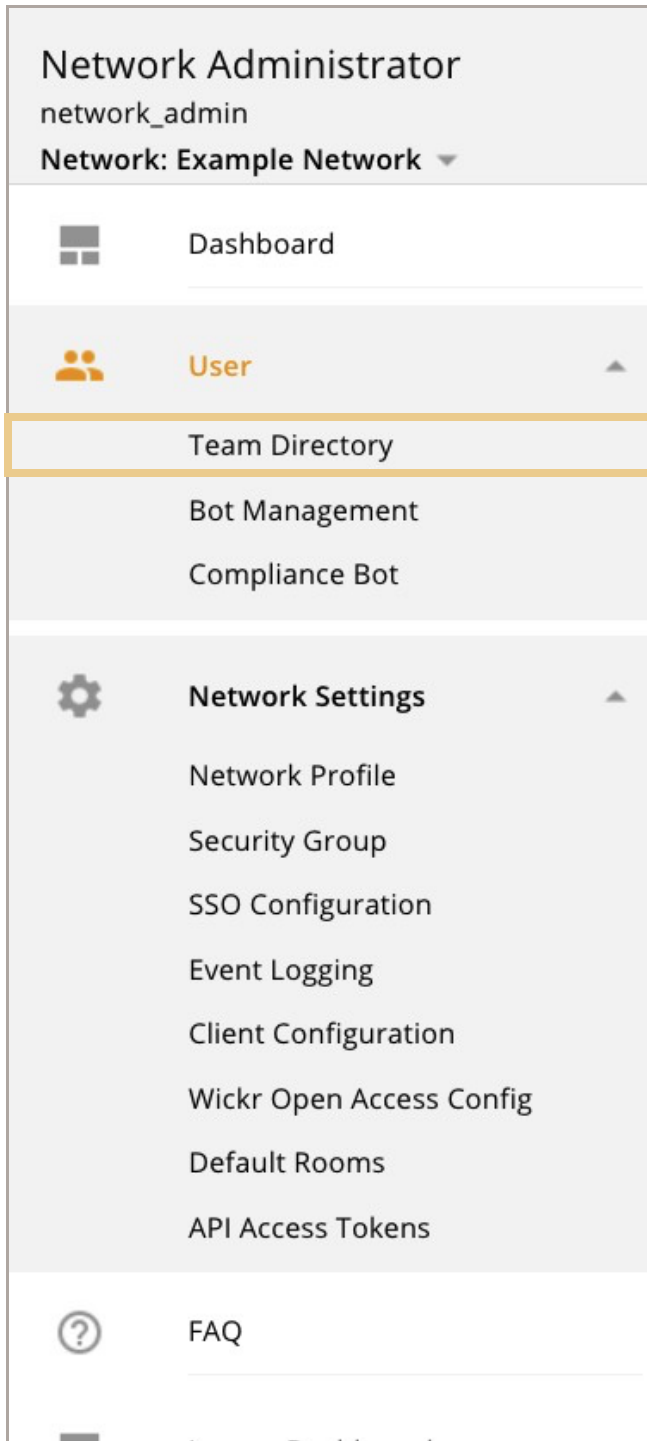
Creating a user manually requires the following information:

- **Email or Username:** If using Global Federation this must be in email format.
- **Password:** Up to 128 characters. All characters allowed, including spaces.
- **Security Group:** Can be changed anytime later.

Additionally, an Administrator can set a visible first and last name. This will be shared with any contact across any internal network.

- **First Name**
- **Last Name**





# Inviting Administrators

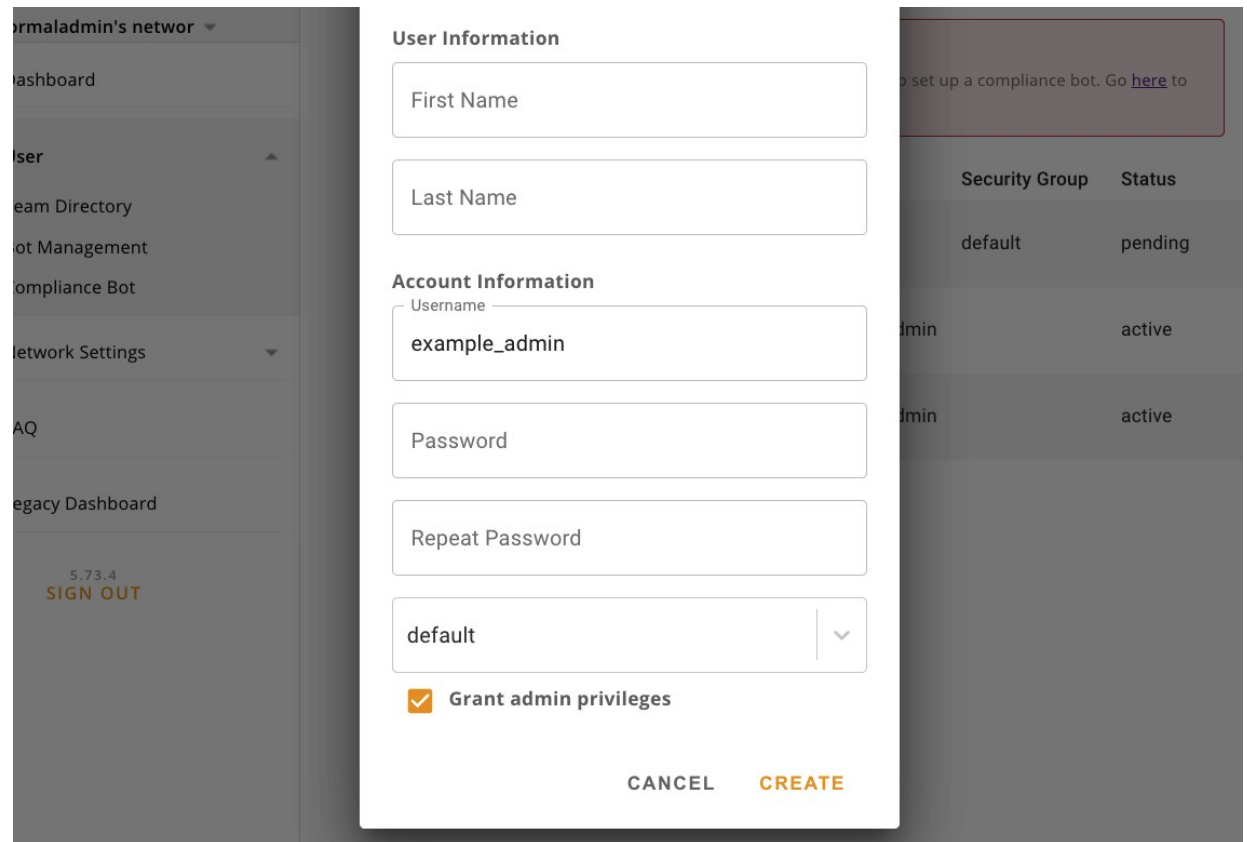
Network Administrators can add any already existing Administrator to a Network they manage. Network Administrators cannot create brand new Administrators.

Network Administrators can only be created by the Super Administrator.

Use the Create User button to add another administrator to the network. Enter the username of the other admin in the Username field and fill in the Grant Admin Privileges checkbox.

Click Create to invite the admin to your network.

In the image below we're inviting the example\_admin user to this network.

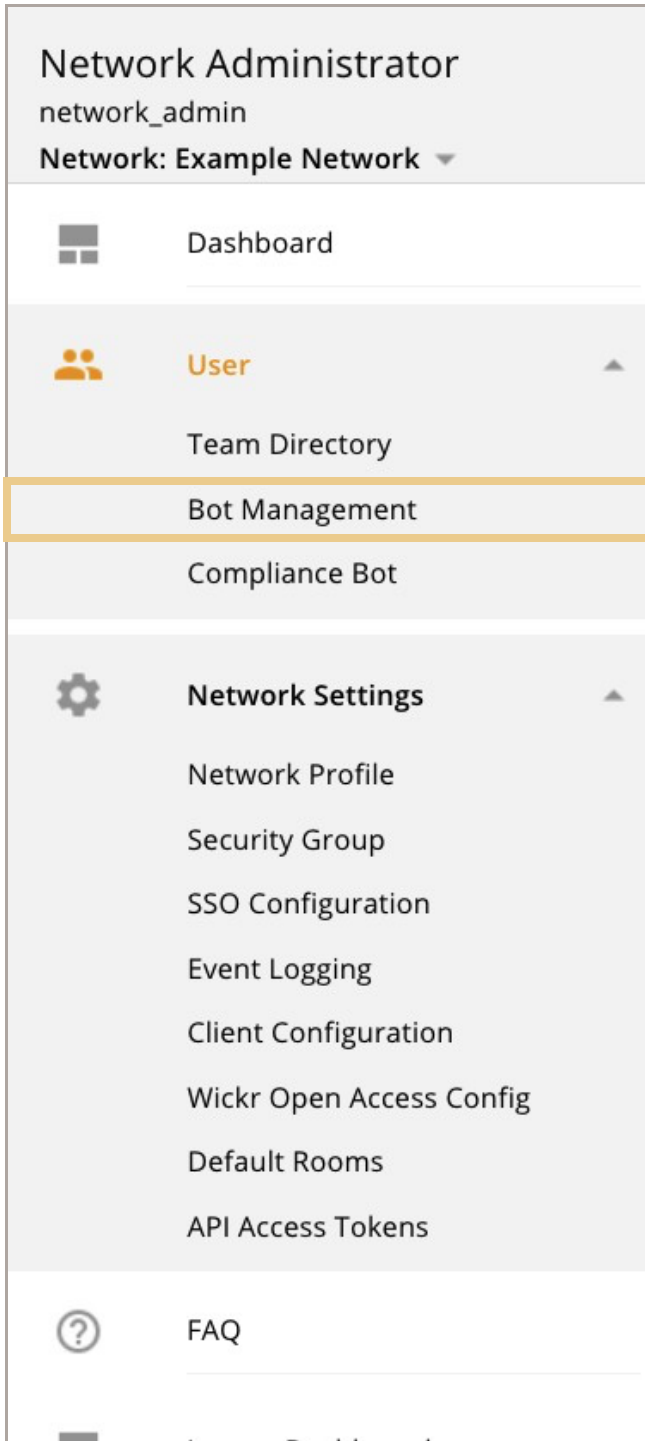


# Accepting Network Invites

Network Administrators can view their invites in the Network dropdown on the upper left of the page.

Clicking the “Join [Network Name]” option will ask the user to confirm.

The image shows a two-part screenshot. On the left is a user profile card for 'Example Administrator' (username: example\_admin) in the 'Example Network'. A 'Join Contractors' button with an envelope icon is highlighted with an orange border. An orange arrow points from this button to a confirmation dialog on the right. The dialog is titled 'Join Network Contractors?' and contains the text: 'You have been invited to join Contractors as an Administrator. Do you wish to accept?'. At the bottom of the dialog are two buttons: 'NO' and 'YES'.



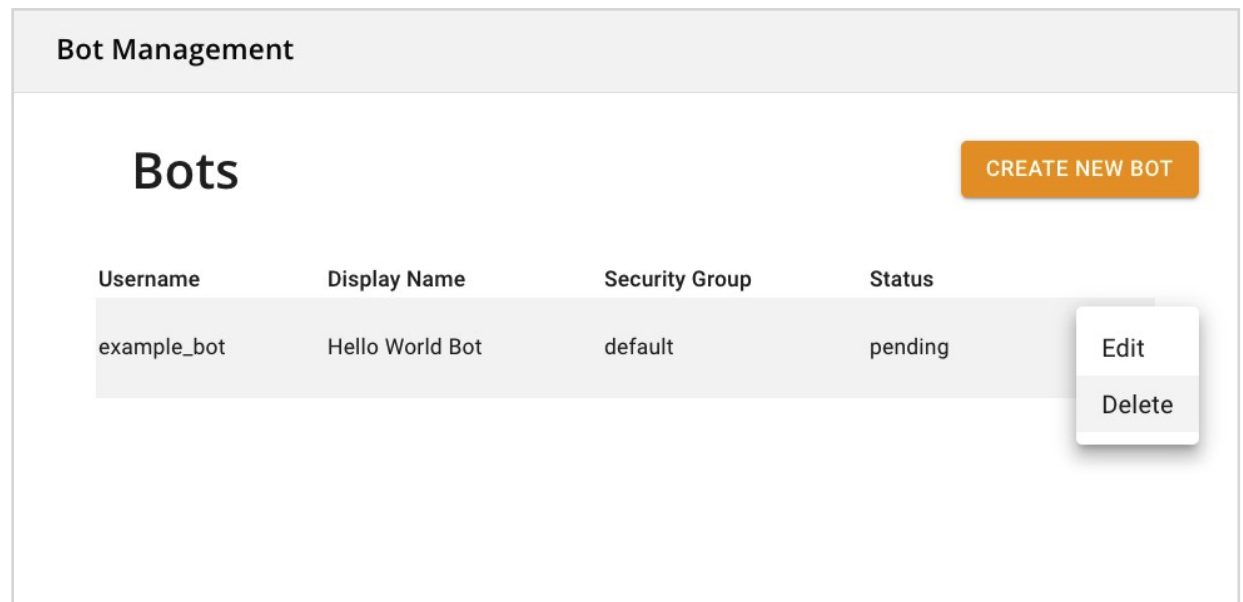
# Bot Management

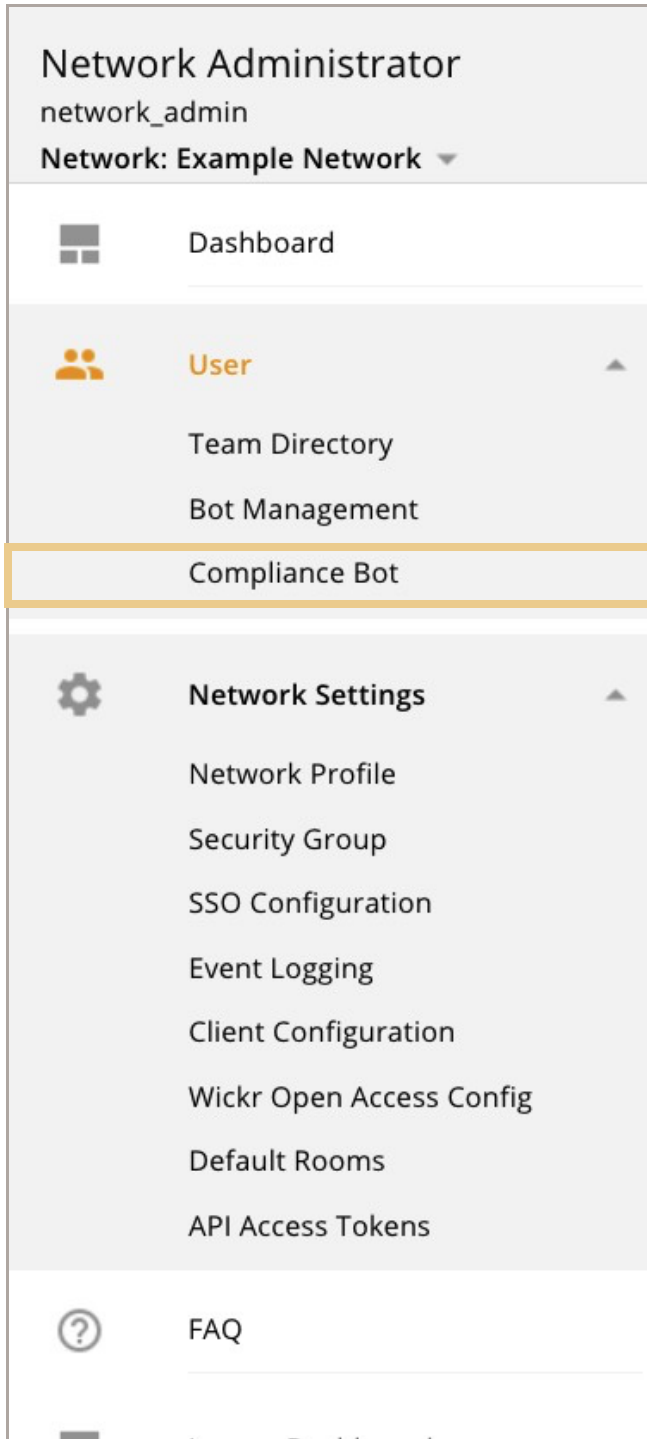
From this screen an administrator can:

- Create a bot
- Delete a bot
- Edit the information of a Pending bot

Username must end with “bot”.

More information can be found here: <https://wickrinc.github.io/wickrio-docs/>





## Compliance Bot

The compliance bot is an additional service only available within Wickr Enterprise.

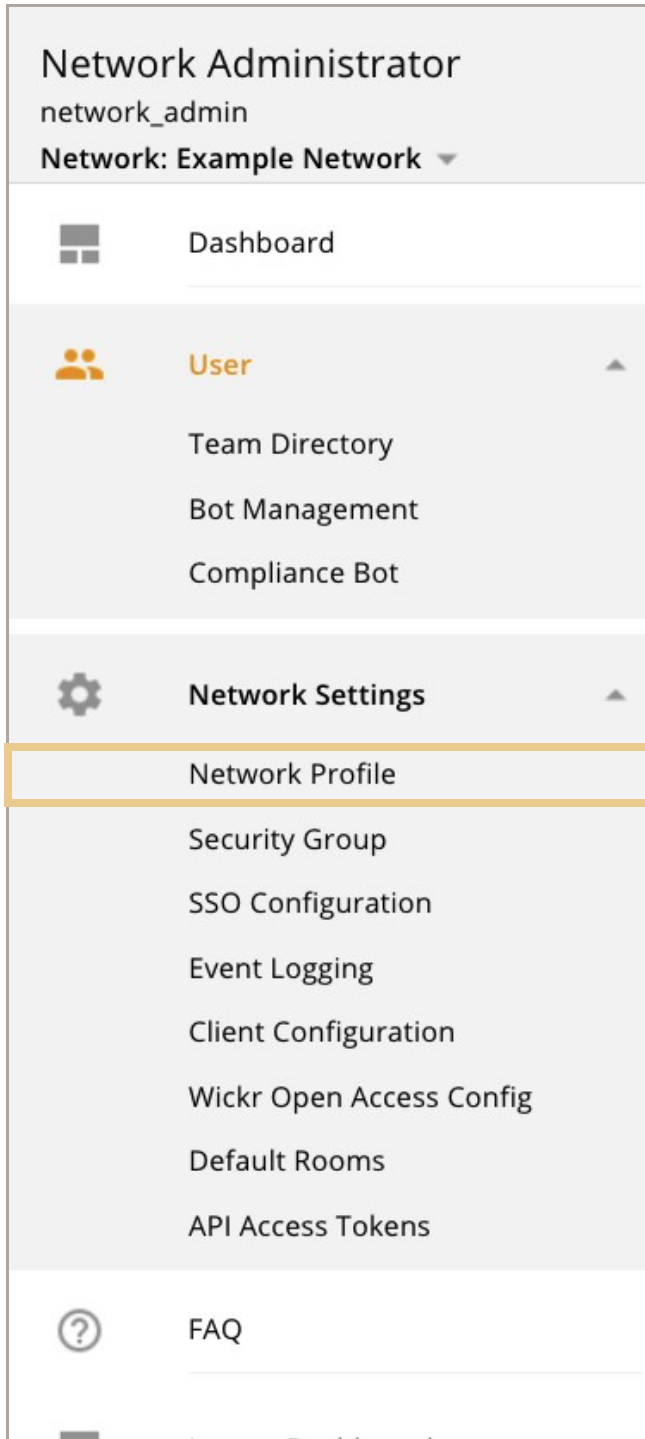
It records every message, attachment, and specific metadata sent within or from the Network. It does not record information sent **into** the network.

This is achieved by adding a bot to the network before users are provisioned. Once the bot is running, configuration files will have compliance information that facilitates the message archiving process when users begin to register and use the app.

More information about the Compliance Bot can be found in the document:

[\*Compliance Service Deployment Guide\*](#)

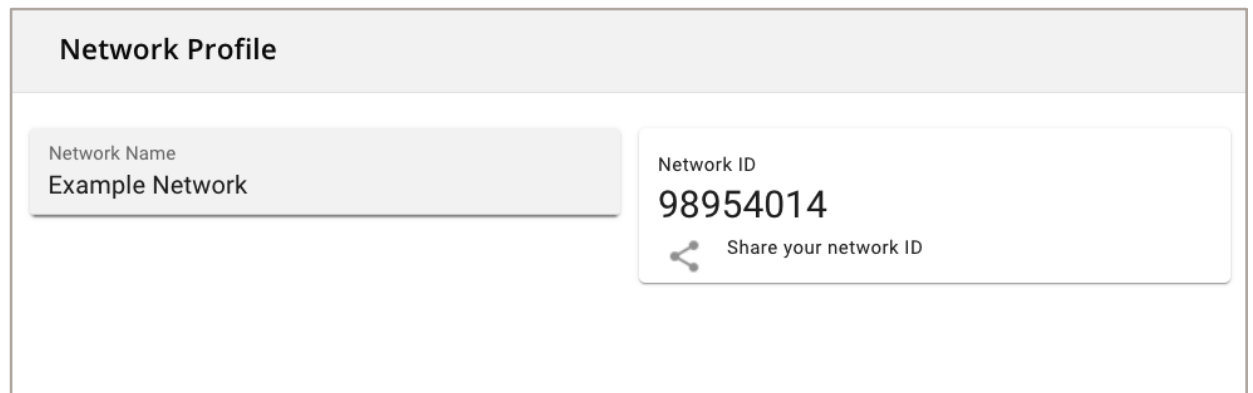
A screenshot of the 'Compliance Bot Setup' form. The form has a title 'Setup' and a sub-header 'Compliance Bot'. Below the title, there is a paragraph of text: 'To create your compliance bot, you will need to set up a username and initial password. Once created, the bot will be inactive until the Docker image is started & configured.' There are three input fields: the first is labeled 'compliance\_bot' and contains the text 'compliance\_bot'; the second and third are password fields, both containing six dots. At the bottom right of the form is an orange 'SUBMIT' button.



## Network Profile

The network profile screen allows an Administrator to set the name of the network, which is visible to all users within it, and also displays the Network ID.

The Network ID is needed when using Federation with other networks.



Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration**
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens
- FAQ

# SSO Configuration

The SSO Configuration page allows an Administrator to add SSO authentication to a specific network. If using ADFS it is also possible to sync Wickr Security Groups with Active Directory user Groups.

- **Network Endpoint:** This is the URL of the Enterprise endpoint to enter into your SSO system. This is pre-filled based on the supplied install hostname and may not be what your physical networking requires.
- **SSO Configuration:** These options are what Enterprise will use to connect to your SSO system.

Notably, the Company ID value will be visible to end users during registration. This ID must be unique as it is used to point the Enterprise client to the specific SSO resource.

- **Security Group Synchronization:** When SSO is configured with an ADFS or openLDAP system, this will allow the local Enterprise Security Groups to be synchronized with an OU on the ADFS side.

### Single Sign-on & LDAP Configuration

#### Network Endpoint

Wickr endpoint to use on your SSO IDP side to connect to Wickr.

Redirect URI	https://107. .65/deeplink/oidc.php	<b>COPY</b>
--------------	------------------------------------	-------------

#### SSO Configuration

SSO provider connection details

**START**

#### Security Group Synchronization

Works best with ADFS 4.0+ on Windows Server 2016 or newer.

**SETUP**

Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration
  - Event Logging**
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens
- FAQ

# Event Logging

This changes the default verbosity level for several backend services. It only effects the information in the Admin, Admin-api, Switchboard, and Messaging containers.

- **Activity:** Shows the least amount of information and is the default.
- **IP Address:** Shows the IP address of the sending client in addition to the default level.
- **Messaging:** This shows the most information, which can include:
  - IP address
  - Plaintext username
  - Client ID
  - Device type
  - Recipients

Message contents are never shown regardless of the chosen verbosity.

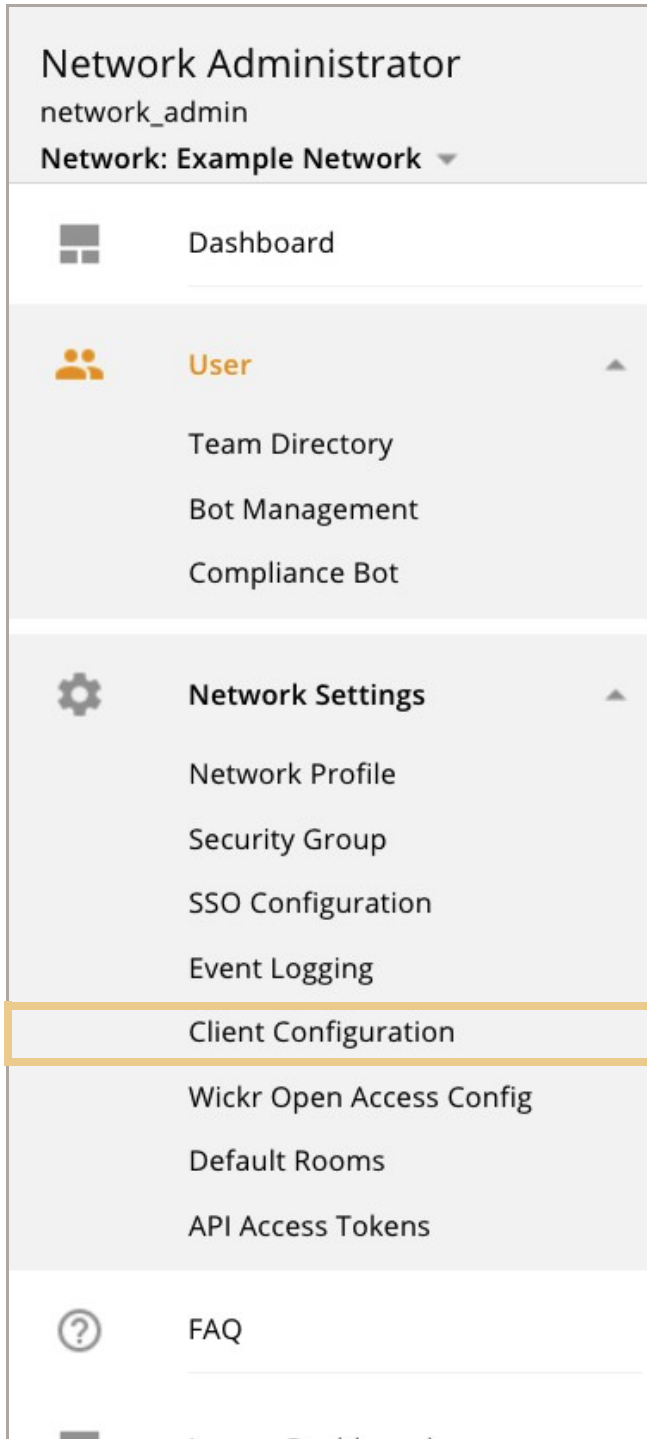
**Event Logging**

Application event logging verbosity level  
This change will affect all logging for this network from this point forward

Messaging ▼ Messaging meta data

- Activity
- IP Address
- Messaging**

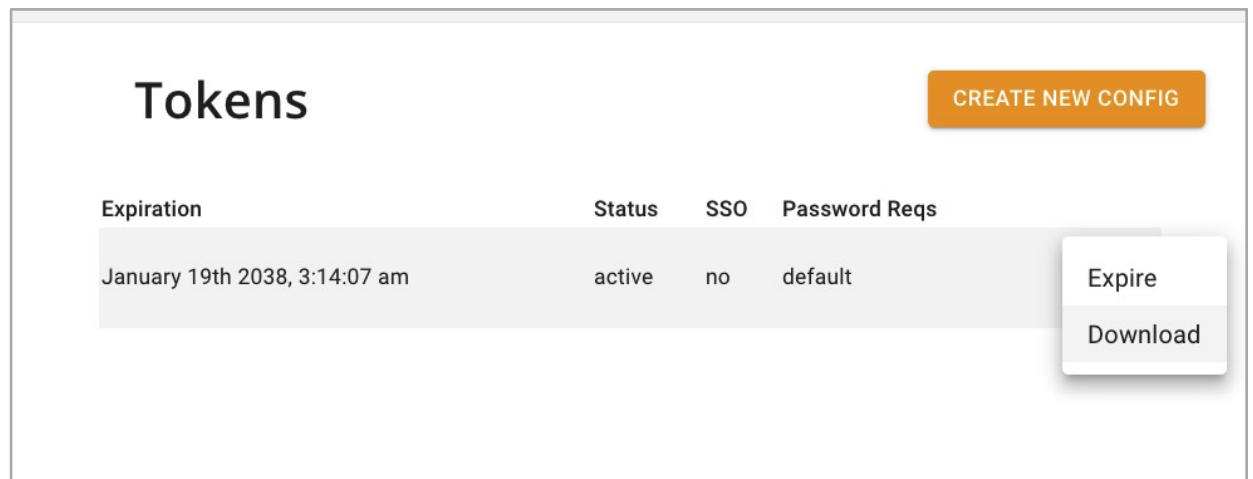




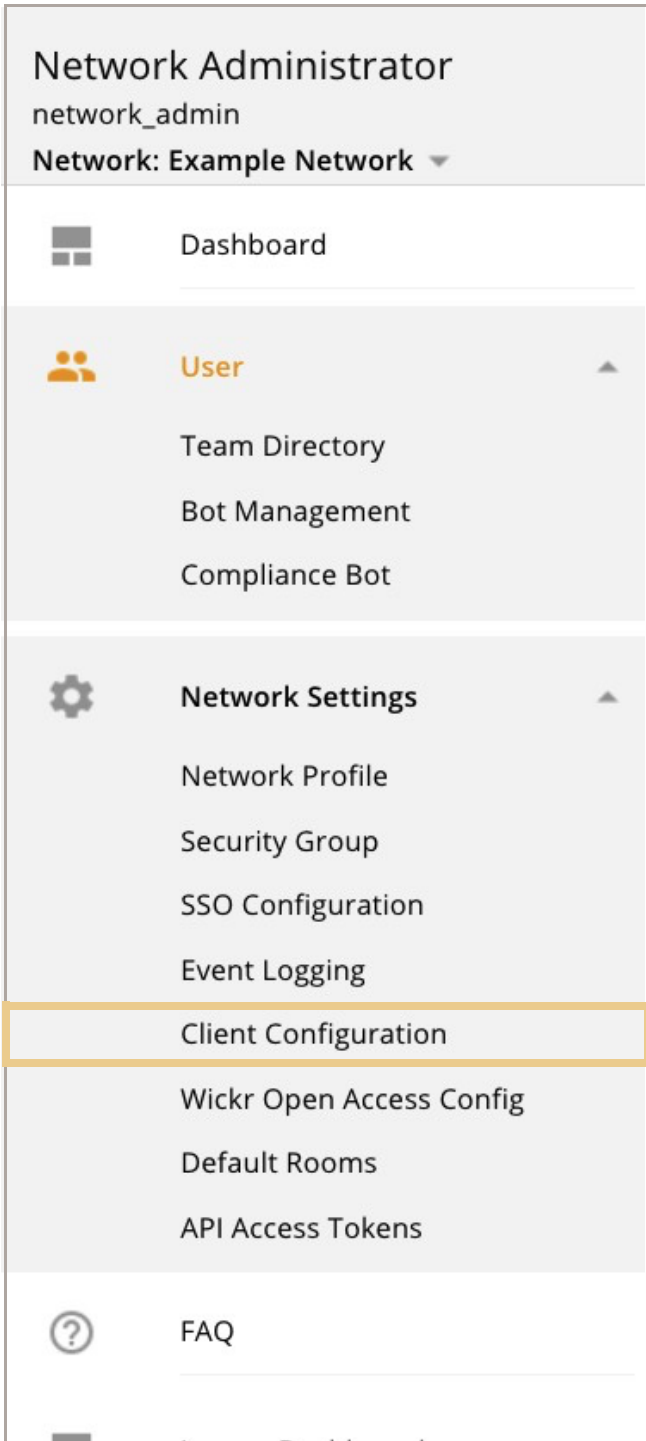
## Client Configuration

In addition to a valid username and password, clients need configuration information to establish a connection to the Enterprise service.

This screen allows the Administrator to create and manage Config Files and Deeplinks which can be shared with users to bootstrap their devices.

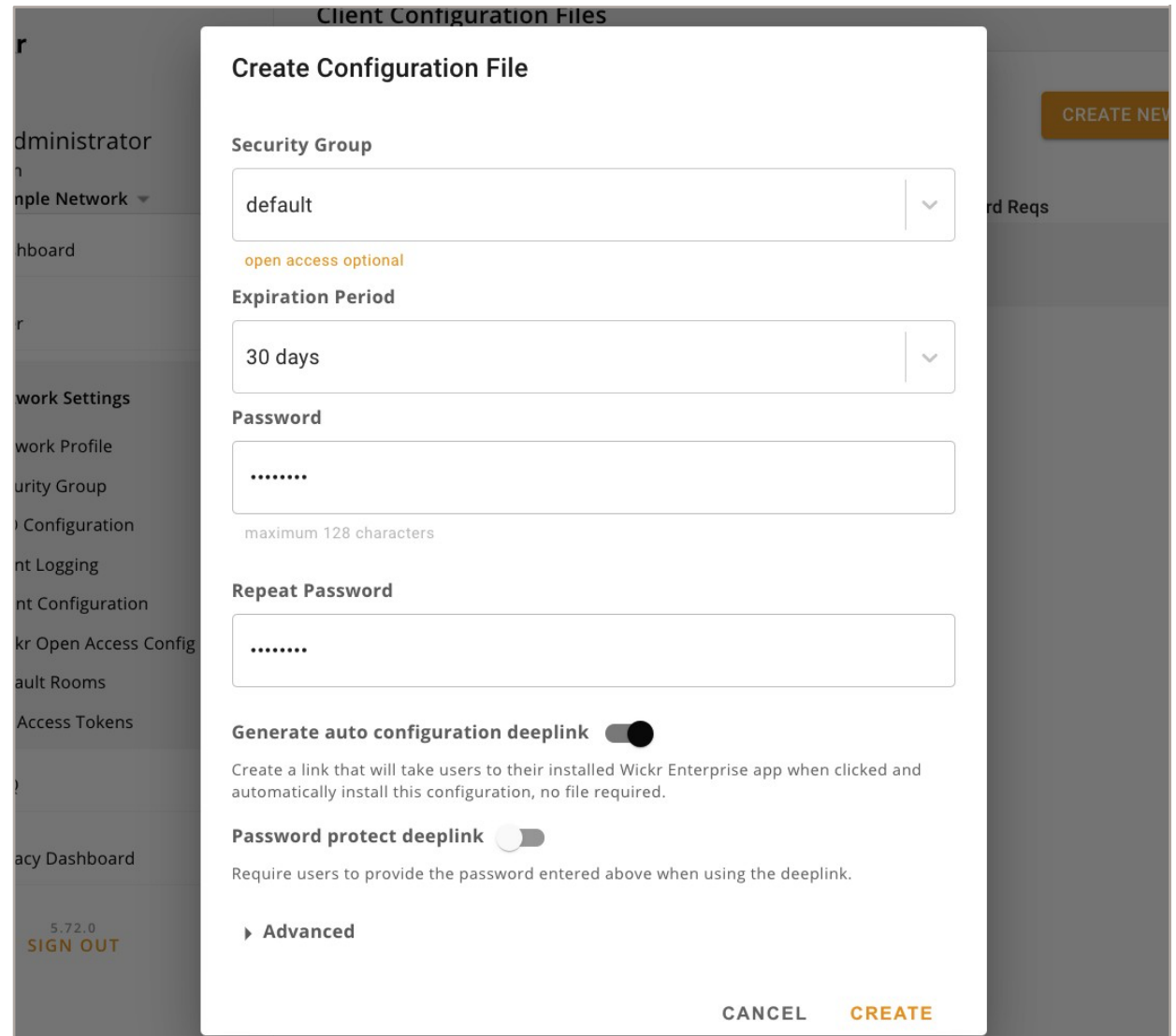


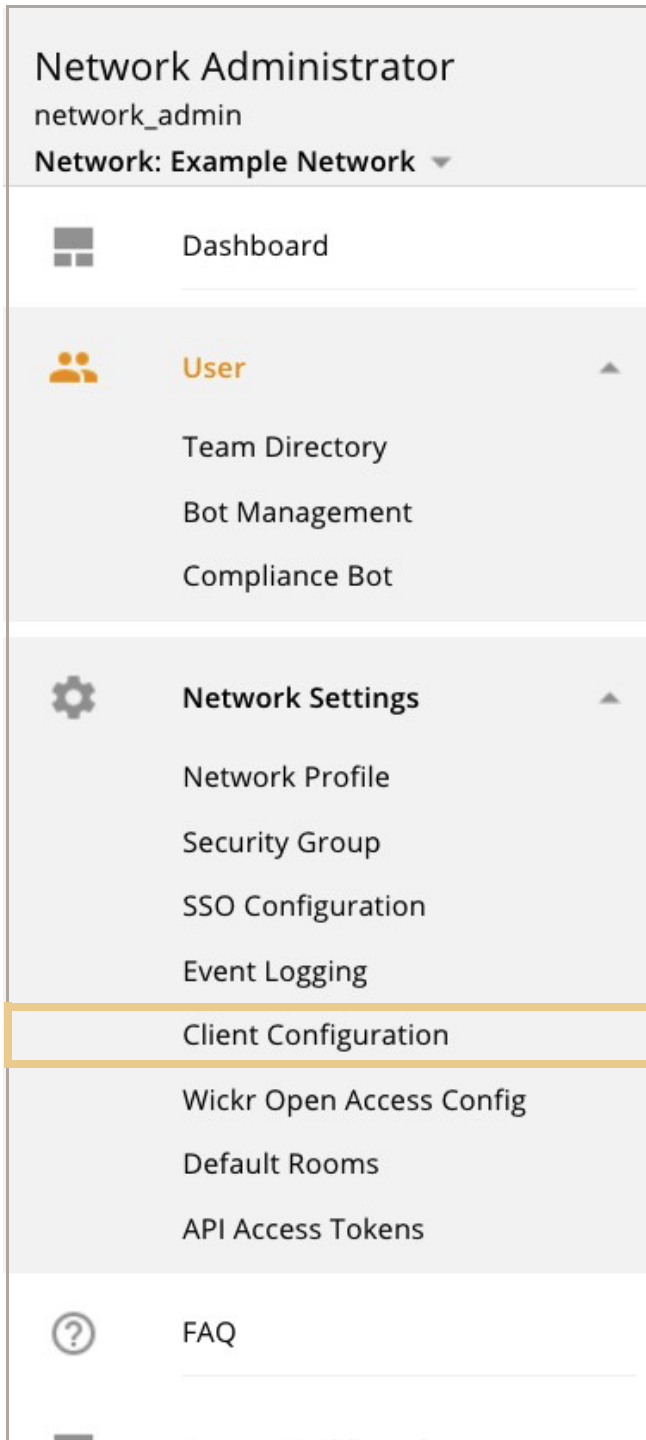
An overview of the creation process is on the next page.



Config Files must be encrypted with a password.

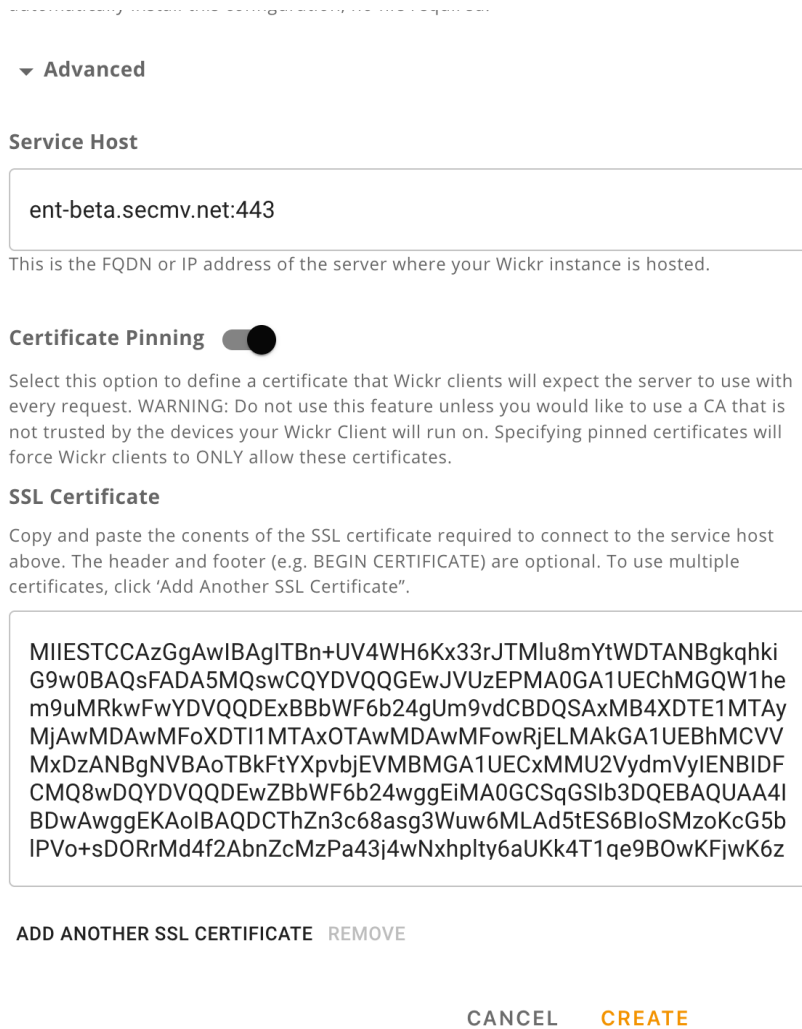
Deeplink passwords are optional.

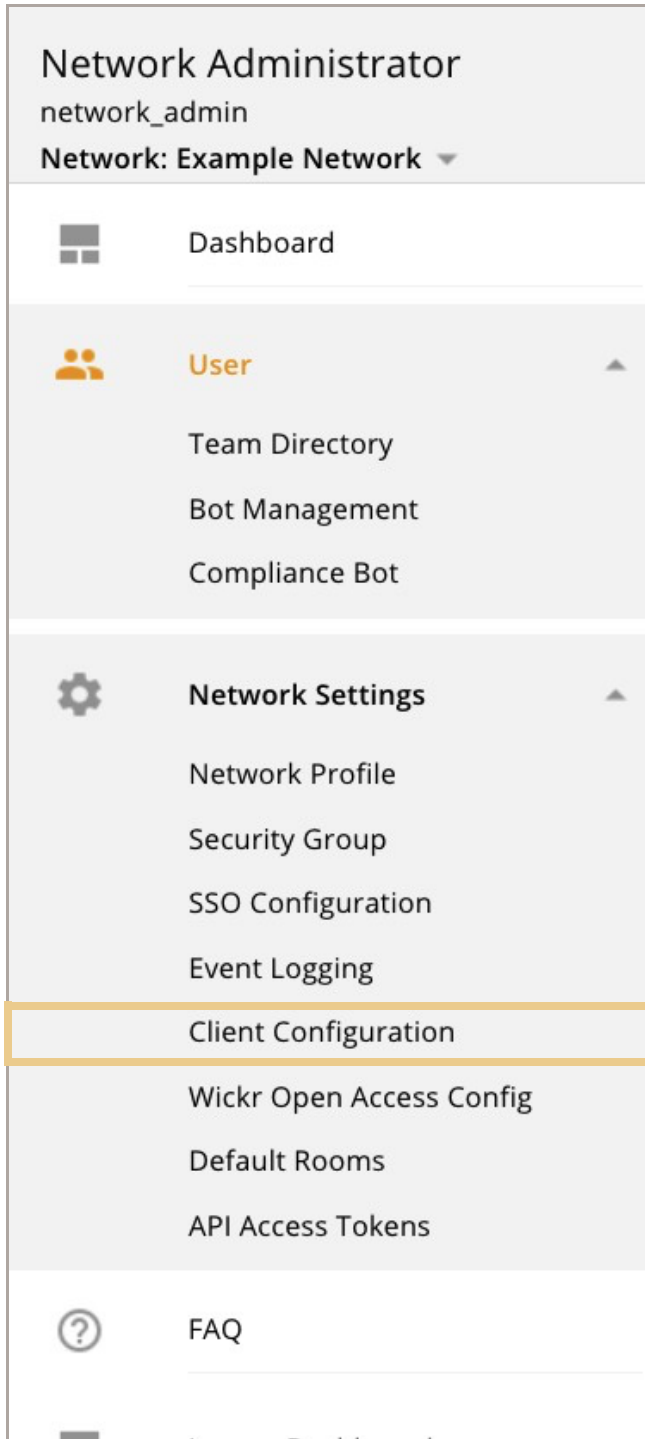




Certificate pinning can be configured by expanding the Advanced options. If pinning is selected, Wickr clients will ONLY trust and connect to Enterprise service hosts which present the specified certificate(s). If pinning is unselected, clients will use standard, platform-based certificate validation when connecting to their Enterprise host.

Note that client platforms can vary in what they consider to be valid X.509 certificates. If you plan on using a private certificate (i.e., certificates not obtained from a Digital Certificate Authority), we strongly recommend that you enable certificate pinning to ensure that your certificate is trusted on all client platforms.

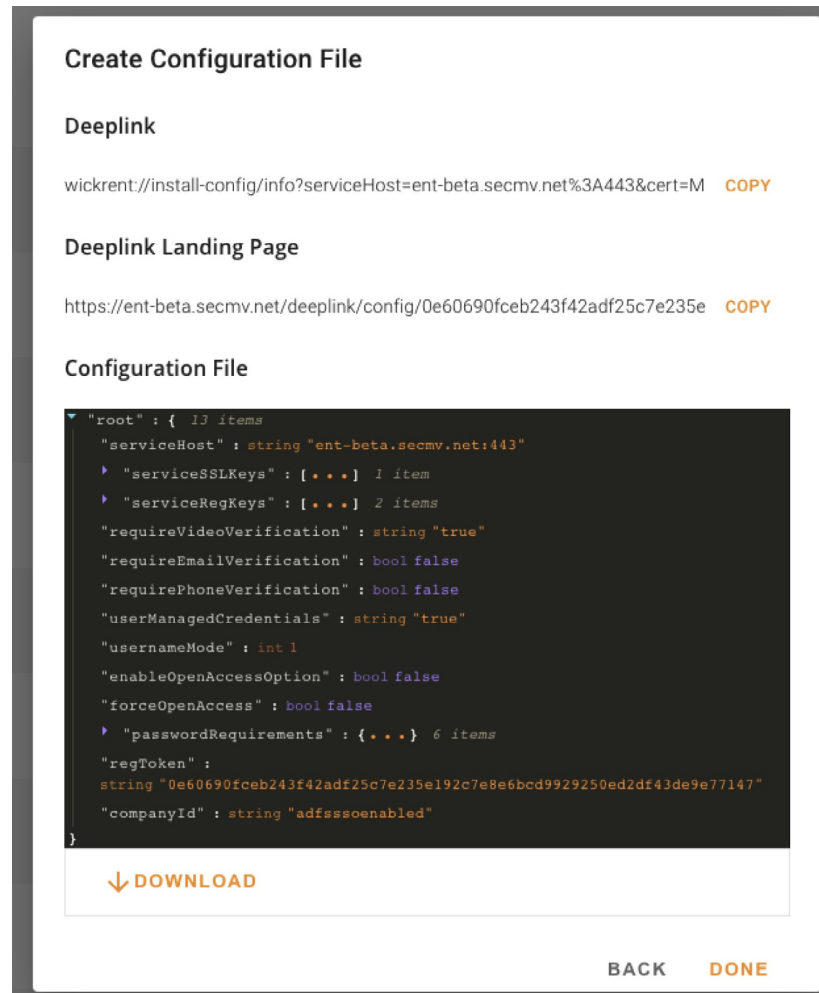




After creating the configuration file, a Deeplink URL and a Deeplink Landing Page URL will also be created.

The Deeplink is a url that will launch the app directly (on desktop, iOS, and Android) but may not be directly usable on a mobile client. For security reasons many mobile mechanisms for rendering that link will block it.

The Deeplink Landing Page is a url that any user can access from any normal mechanism. This is the url that should be distributed if the company is not hosting their own internal website for the config file.



Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config**
  - Default Rooms
  - API Access Tokens
- FAQ

## Wickr Open Access

Wickr Open Access is an additional layer of network obfuscation that uses various connection methods deployed through our partner Psiphon.

This is not a default service and requires an additional license provided by Wickr.

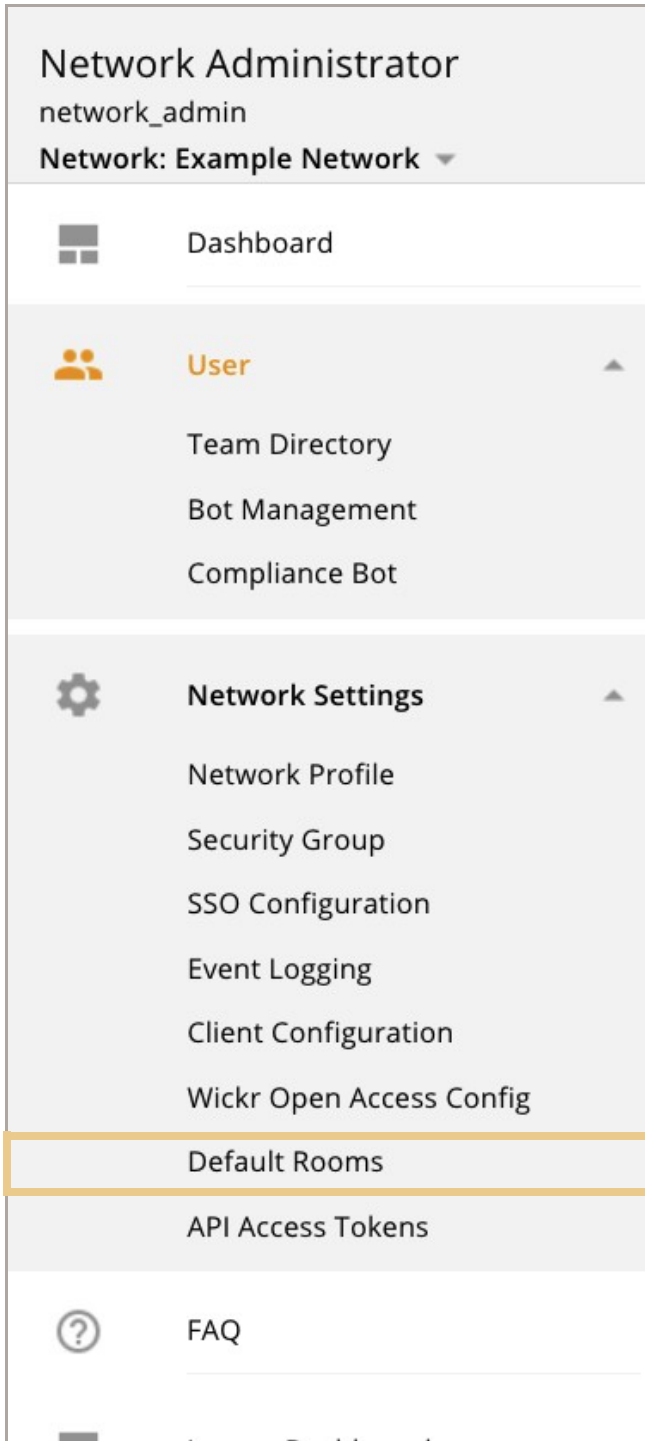
If enabled, it can also be forced on for every user in a security group.

**Wickr Open Access Configuration**

**Wickr Open Access** SAVE CLEAR

In order to use Wickr Open Access, you must enter your configuration license below.

Configuration License



## Default Rooms

When the Super Administrator has enabled this option it allows Network Administrators to create rooms managed by a Bot. This Bot will automatically add users to a room. The users will be re-added if they leave.

A room can be made for all users in the network, for specific Security Groups, or both.

In these rooms there are no other moderators other than the Default Room Bot so settings and users can't be managed within the app by End Users.

### Network Room

All users in this network will automatically be put in this room. Be careful when using this with large networks.

Title

Description

Message Expiration

Messages in this room will be deleted for all users after this time.

Message Burn On Read

Messages in this room will be deleted for all users after this time.

CREATE A ROOM FOR THIS GROUP

INACTIVE

### Security Group: default

Users assigned to this security group will automatically be put in this room.

Title

Description

Message Expiration

Messages in this room will be deleted for all users after this time.

Message Burn On Read

Messages in this room will be deleted for all users after this time.

CREATE A ROOM FOR THIS GROUP

INACTIVE

Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group
  - SSO Configuration
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens**
- FAQ

# API Access

The API Access Token page allows an Administrator to manage API Tokens.

Tokens only need a label when created. These tokens can be revoked at any time.

## Tokens

Create tokens for access to admin API REST endpoints. [Endpoint Documentation](#) CREATE API KEY

API Key	Label	Created	Last Accessed	IP Address	User Agent

Complete API documentation is available within the Admin Panel. No online access is needed and examples can be generated to quickly test an endpoint using curl.

**directory** ▾

**GET** /network/{networkId}/directory/userCount

get the number of users in a network

**Responses**

**Curl**

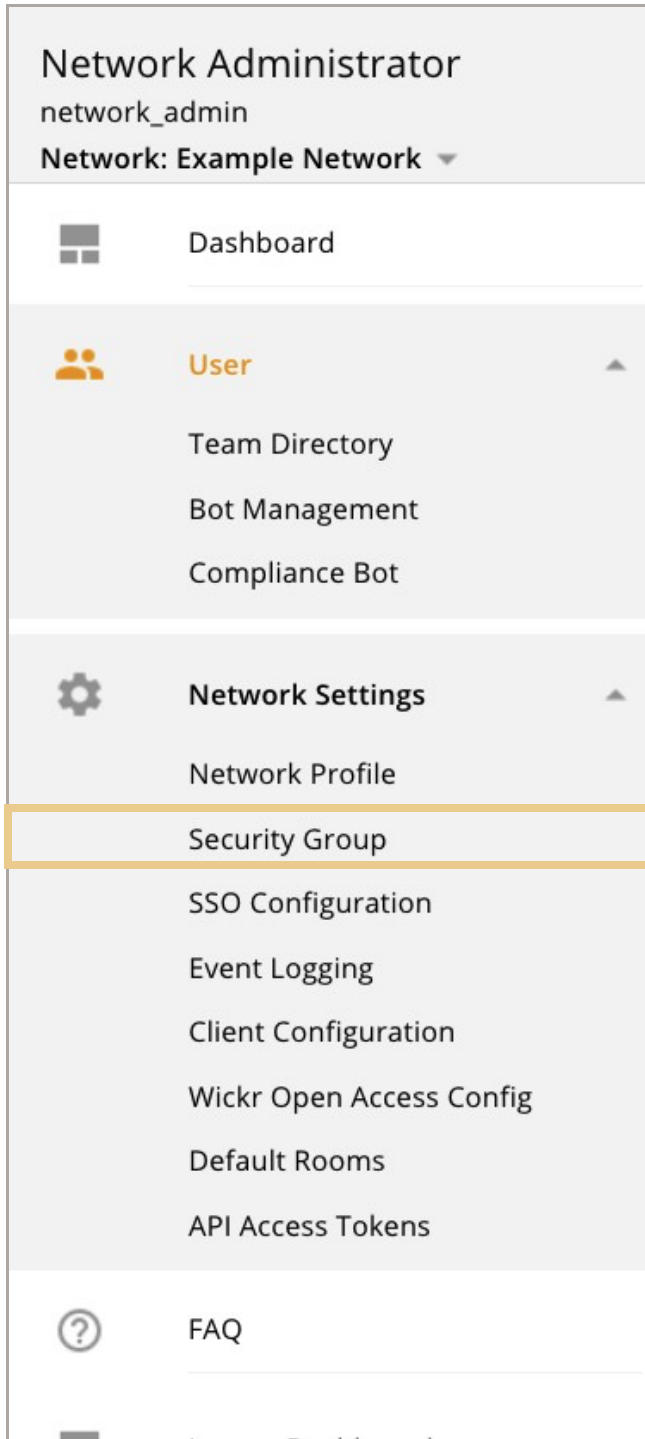
```
curl -X GET "https://107.21.236.65/admin-api/network/76232813/directory/userCount" -H "accept: application/json"
```

**Request URL**

```
https://107.21.236.65/admin-api/network/76232813/directory/userCount
```

**Server response**

**Code**    **Details**

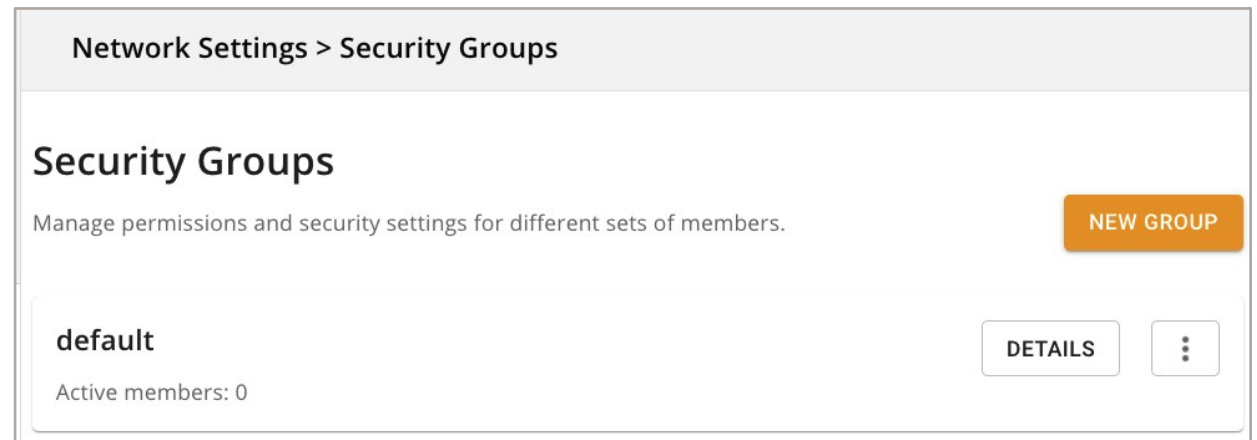


# Security Groups

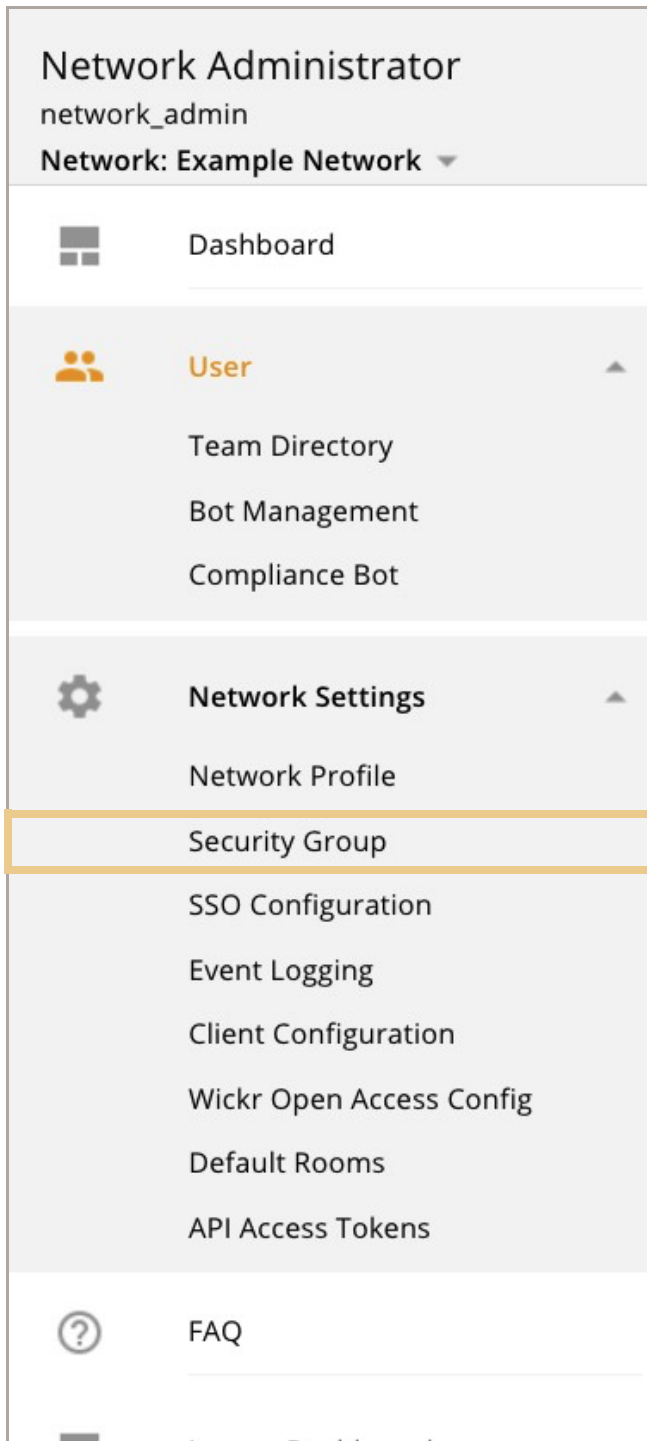
Security Groups are the basis for any features available and security controls that apply to a group of users. There is always at least one Security Group in a Network. It is the Default security group with the Wickr standard recommendations.

Up to one hundred Security Groups can be made in a single network.

The overview page will show any available groups and how many users are in each one.



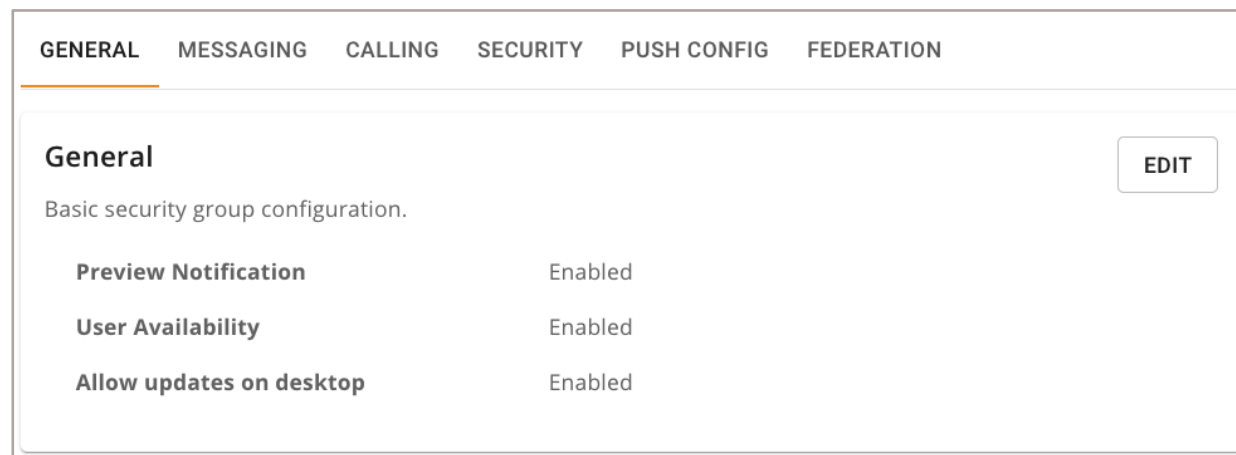


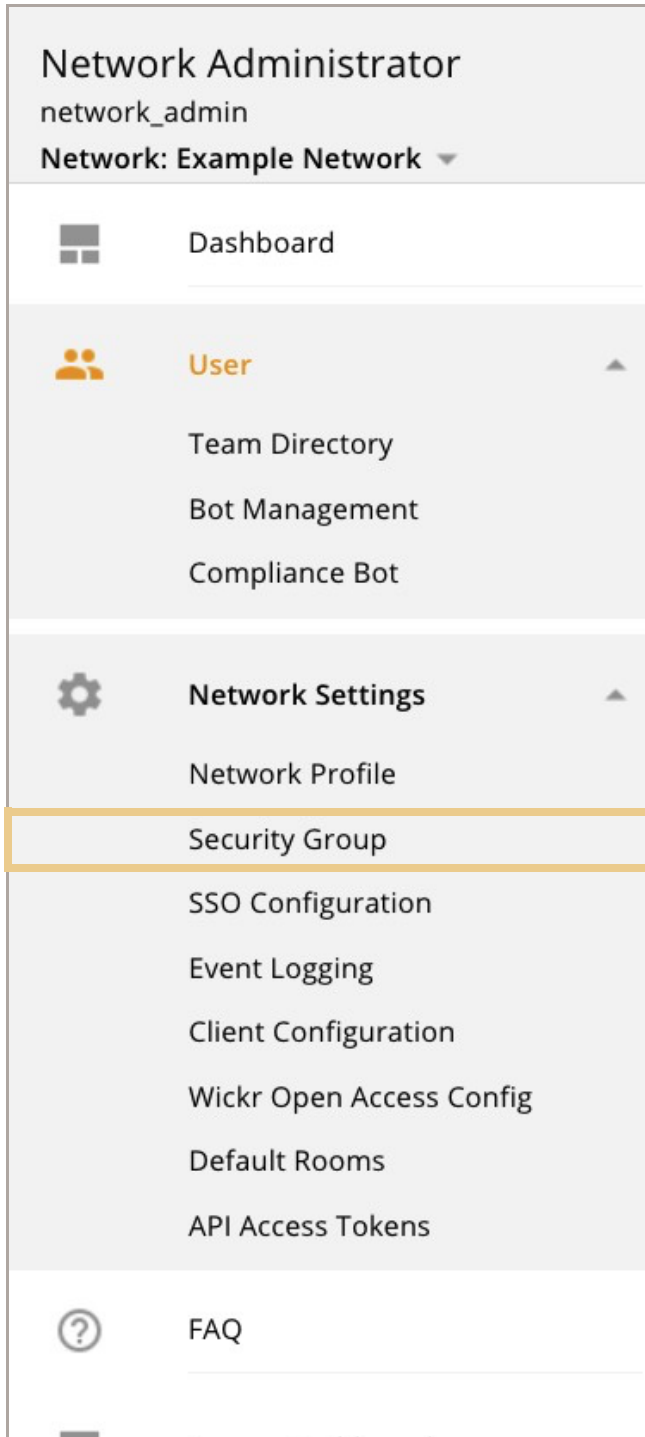


## General

The general tab has three available options:

- **Preview Notification:** If enabled on both the server and client this will allow users' new message content to be previewed in any notifications. If disabled they will only display who the message is from or the room/group name.
- **User Availability:** Allows users to enable "Show my Status" Presence in the app.
- **Allow updates on Desktop:** Displays a banner on Desktop (Windows & macOS) clients when there is an update available.

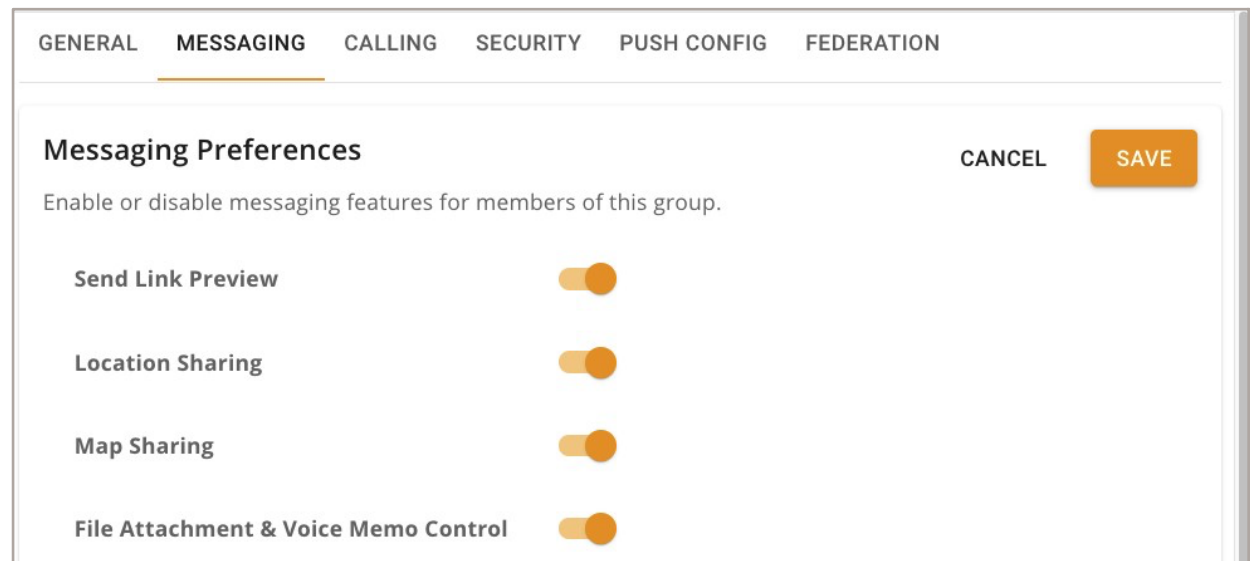


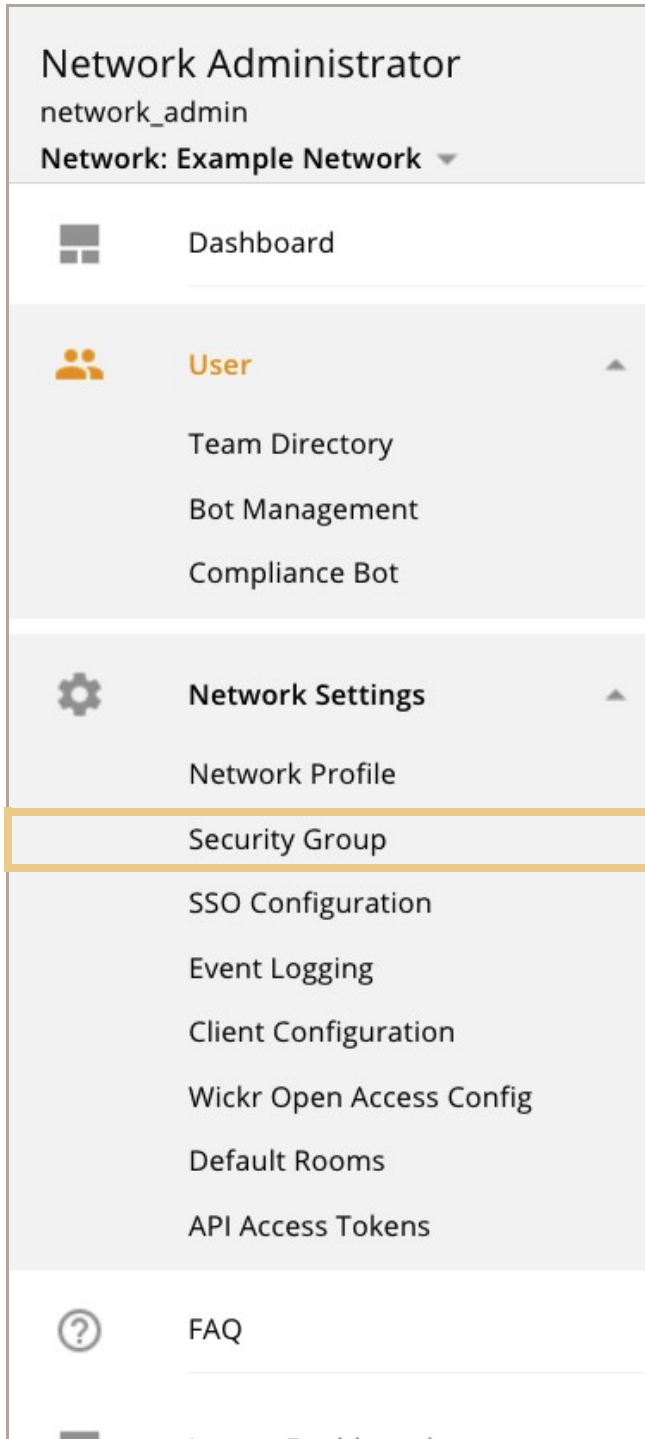


# Messaging

The messaging tab has the following available features for users:

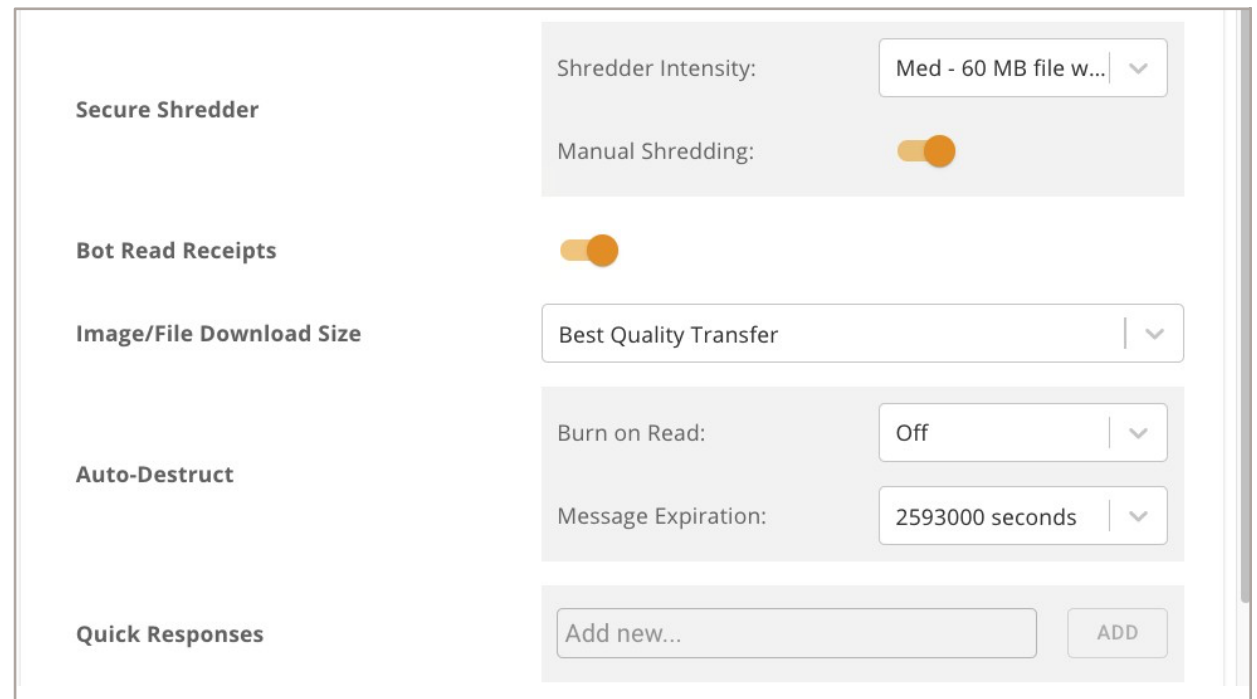
- **Send Link Preview:** This allows a user to send or receive previews for URLs sent within Wickr. The preview is generated from the sending device. Recipients will not connect to the underlying URL until clicked.
- **Location Sharing:** Allows users to share a link to their GPS coordinates in the app.
- **Map Sharing:** If enabled alongside Location Sharing, it will allow a user to send a map with their location on it. This map can be shared for a pre-determined amount of time that will update as the user moves.
- **File Attachment & Voice Memo:** If this is disabled, users will be unable to send attachments or voice memos. This also prevents downloading attachments sent by others in rooms, groups, or DMs.

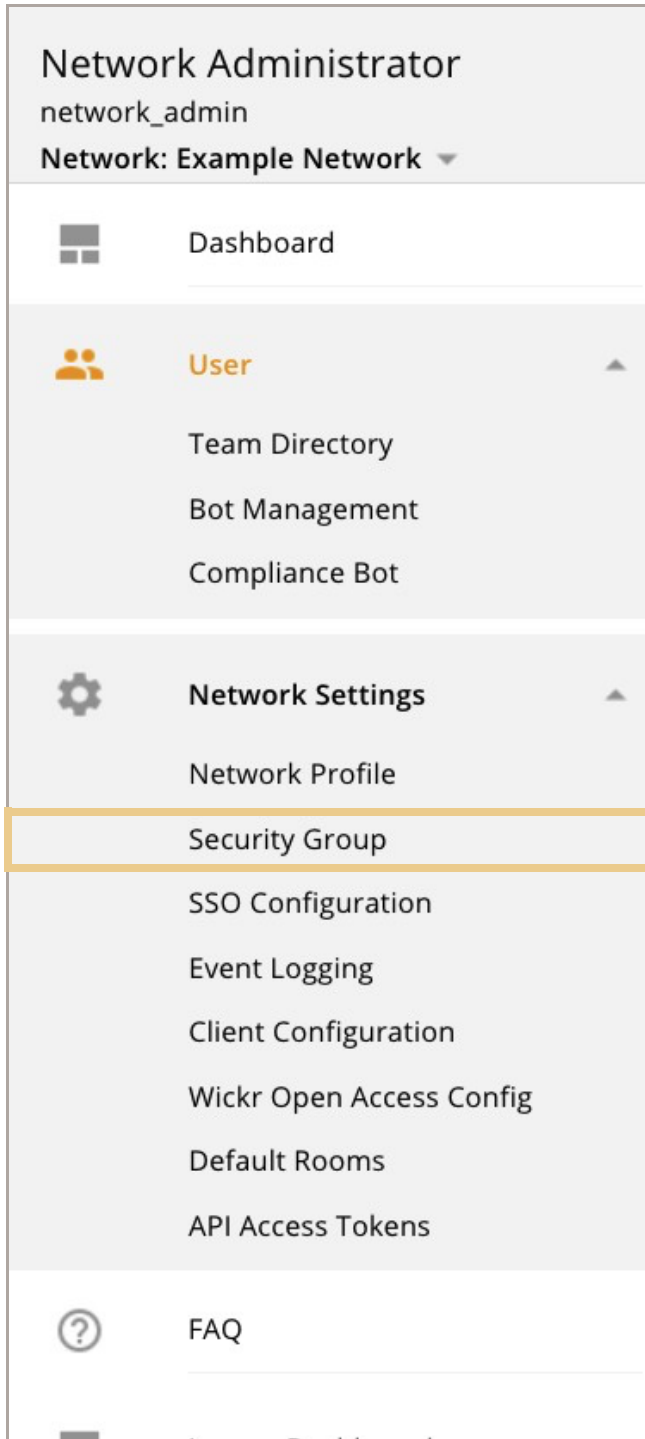




The messaging tab also has these additional features:

- **Secure Shredder:** The Wickr shredder will write random data over any RAM and Disk Space used by files opened in the app. This does not apply to files exported, only files opened in a preview within the Wickr apps.
- **Bot Read Receipts:** Allows bots to automatically “read” messages in a room instead of requiring users to @ the bot for interaction.
- **Image/File Download Size:** By default will upload and download the file uncompressed. If compression is enabled the Apps will attempt to compress the data before encrypting and uploading.
- **Auto-Destruct:** This is the default **maximum** for any message sent within the network. Users can adjust to any amount lower than this value.
- **Quick Responses:** Allows administrators to set pre-filled messages that users can send by clicking within the app. Each quick response supports up to 8,000 characters, including formatting and emoji. Only **ten** are allowed per group.

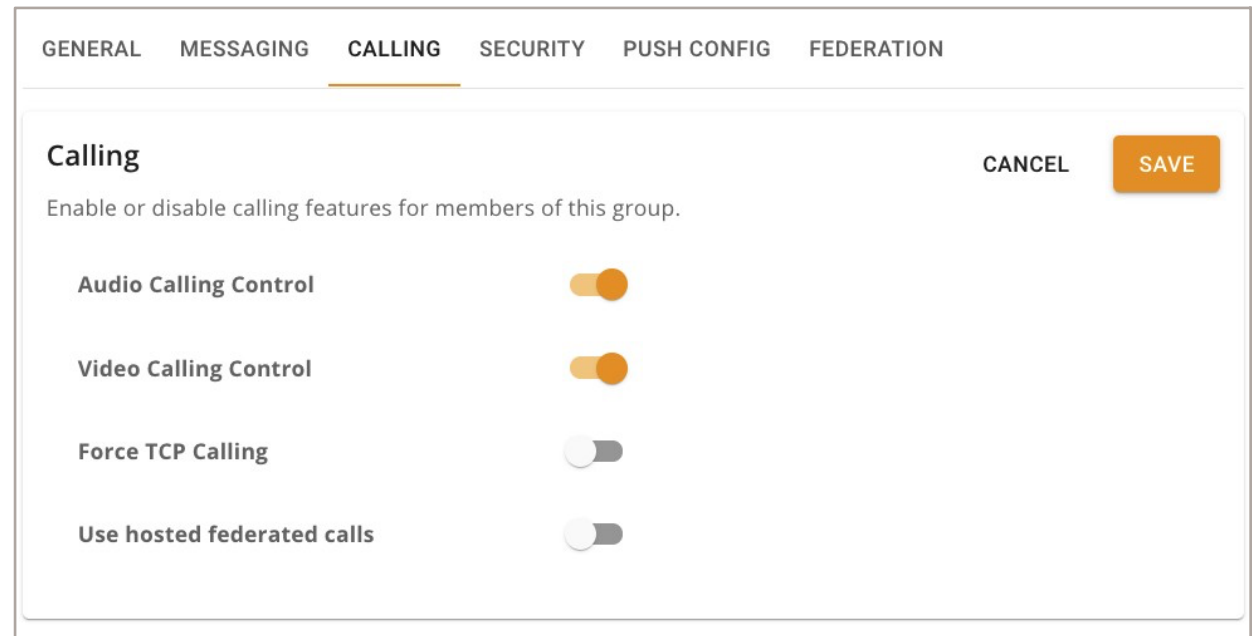


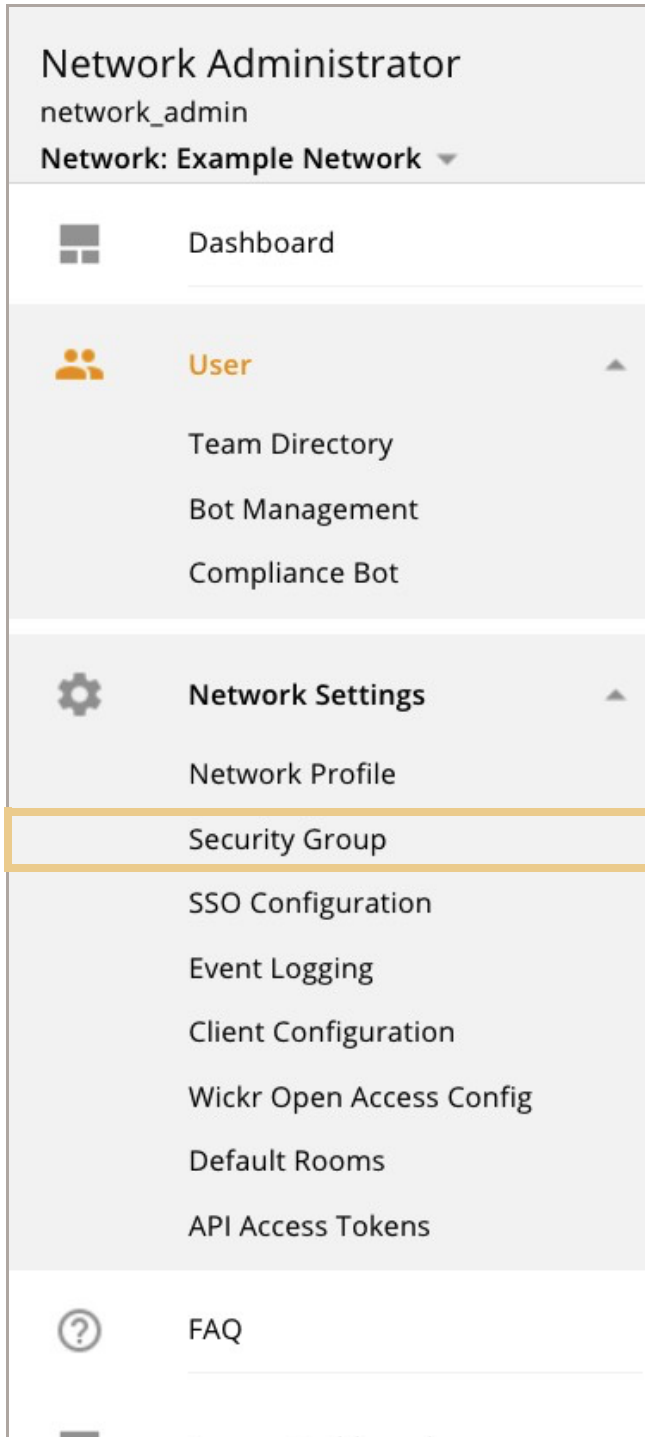


# Calling

The calling tab has the following available features for users:

- **Audio Calling Control:** This disables calling for users. At a minimum users must be able to share audio to start or join a call. Enabled by default.
- **Video Calling Control:** If disabled users cannot share their camera feed or their screen. Enabled by default.
- **Force TCP Calling:** This forces users to connect to calls over TCP instead of the default UDP connection. Clients will try UDP first and then fall back to TCP automatically, but this will save time for users if UDP is known to be blocked.
- **Use Hosted Federated Calls:** For Global Federation. Disabled by default. If this is enabled it will have users connect to the remote infrastructure for calls. This means Enterprise users will join the Me, Pro, or remote Enterprise calling infrastructure instead of the local servers. Useful for locked down environments where outside users can't connect to local or internal infrastructure.





# Security

The security tab has the following available options for administration:

- **Always Re-authenticate:** This forces mobile users to enter their password or biometric auth when bringing the app to focus. Disabled by default.
- **User Password Permission:** If this is disabled users will be unable to change their password during registration and after activation. Enabled by default.
- **Password Complexity Requirements:** This forces users to follow specified criteria when creating a password during registration and when changing their password.
- **Device Reset:** The number of bad login attempts before the device is reset.
- **User Account Suspension:** If a user continues to enter the wrong password, it will suspend the account after this amount of tries.

## Security CANCEL SAVE

Configure additional security features for this group.

**Always Re-authenticate**

**User Password Permission**

**Password Complexity Requirements**

Minimum password length:

Lowercase letter:

Uppercase letter:

Number:

Special character:

**Device reset**

**User account suspension**

Network Administrator  
network\_admin  
Network: Example Network ▾

- Dashboard
- User** ▲
  - Team Directory
  - Bot Management
  - Compliance Bot
- Network Settings** ▲
  - Network Profile
  - Security Group**
  - SSO Configuration
  - Event Logging
  - Client Configuration
  - Wickr Open Access Config
  - Default Rooms
  - API Access Tokens
- FAQ

# Push Configuration

The Push Configuration tab has available options for proxy or intermediary networking devices. This can also be used to obfuscate the infrastructure by forcing users to connect to proxies which then forward traffic to the Messaging / App server.

Push Configuration entries supersede any connection information in a config file or deeplink.

- **Messaging Domains:** Domains and IP addresses accepting client connections.
- **Voice & Video Domains:** Domains and IP addresses accepting client calls.
- **Certificate Pinning:** The SSL certificate used during installation is here automatically. We recommend using intermediate certificates here instead of a leaf.

We strongly recommend that you **DO NOT** change certificates or pinning modes here unless you've tested the change on a non-production system. Pushing a certificate that clients cannot validate can render them unable to connect to the Enterprise service with no recourse other than a client reset.

**Messaging Domains** EDIT

List of messaging server domains for push config (max: 100)

ent-beta.secmv.net:443

---

[Download List](#)

**Video & Voice Domains** EDIT

List of voice and video proxy domains for push config (max: 100)

[ None available ]

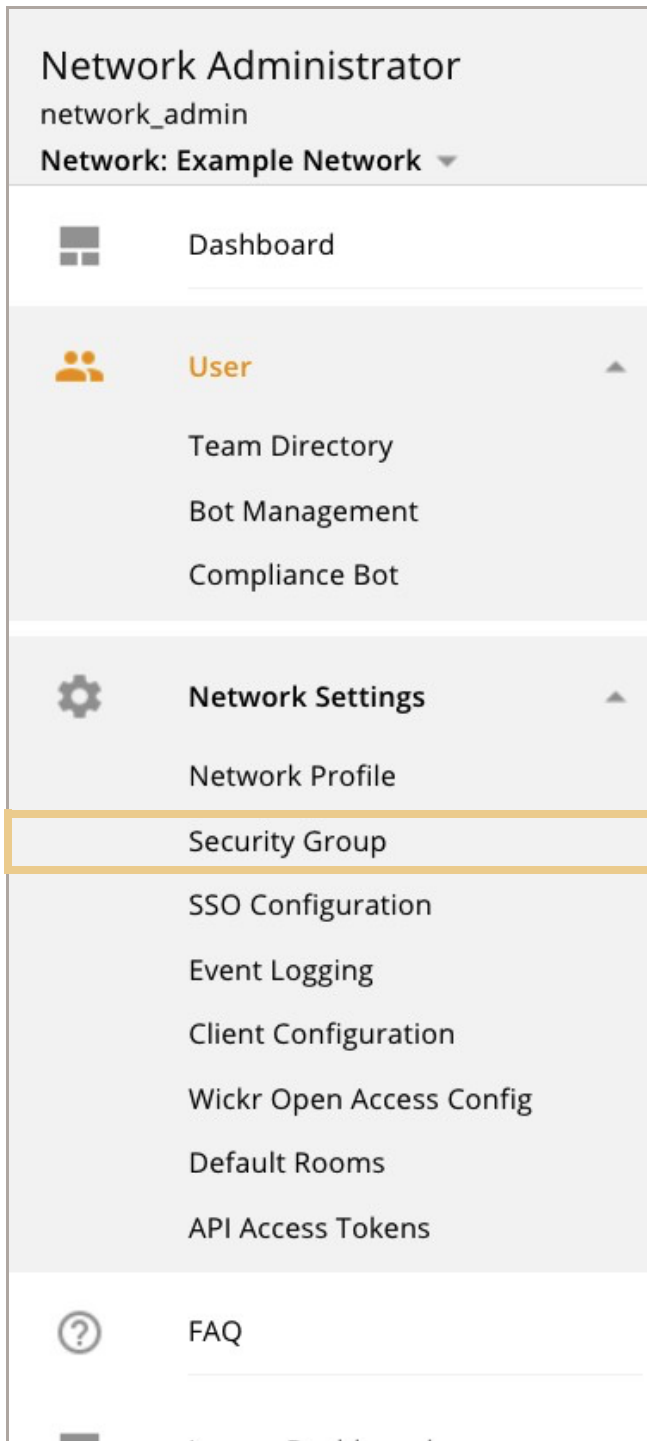
---

[Download List](#)

**Certificate Pinning** EDIT

Certificate Pinning

Select this option to define a certificate that Wickr clients will expect the server to use with every request. **WARNING:** Do not use this feature unless you would like to use a CA that is not trusted by the devices your Wickr Client will run on. Specifying pinned certificates will force Wickr clients to **ONLY** allow these certificates.



## Federation

The Federation tab has available options for communications internal to the Enterprise deployment and external communications with other Wickr Me, Pro, or Enterprise users. External federation only available if the Super Admin provisions.

- **Local Federation:** Available options are Disabled, Enabled, or Restricted.
- **Permitted Networks:** Only shown when “Restricted Federation” is chosen in the Local Federation dropdown. Add labels and Network IDs for other local networks within the Enterprise deployment.
- **Global Federation:** This controls Wickr Me and Pro access if Global Federation has been enabled by the Super Admin. Should not be shown if Global Federation is disabled.

