



Administrator Guide

May 2023

Contents

- Contents..... 2**
- What’s New? 3**
- Common Terms 3**
- Super Administrator 4**
 - Administrator Login 4
 - Super Administrator Settings..... 5
 - Creating a Network Administrator..... 6
 - Manage the Room Bot 6
 - Crash reports 7
 - Registration and Administrator Lockout..... 8
 - Manage Global Federation..... 8
 - Generate API Access Tokens 9
- Network Administrator 10**
 - Dashboard 10
 - Account Settings 11
 - Team Directory 12
 - Inviting Administrators..... 14
 - Accepting Network Invites 15

- Bot Management..... 16
- Compliance Bot..... 17
- Network Profile 18
- SSO Configuration 19
- Event Logging 20
- Client Configuration..... 21
 - Certificate Pinning..... 24
 - Migration to disable certificate pinning 30
- Wickr Open Access Config..... 32
- Default Rooms..... 33
- API Access..... 34
- Security Groups..... 35**
 - General 36
 - Messaging..... 37
 - Calling 39
 - Security 40
 - Push Configuration..... 41
 - Federation 42

What's New?

v5.74	Certificate Pinning: Certificate pinning has been enabled in Enterprise.
v5.73	Admin API has been released! Documentation can be found within API pane. Stability and Bug Fixes
v5.70	Default config file expiration: The default is now 30 days. Global Federation (Pro): Allows communication between Wickr Enterprise and Wickr Pro. Is configured by the Super Administrator.
v5.68	Deeplink generation: Administrators can now provide a link to end users for registration instead of a config file. This can be done on the Client Configuration page. Global Federation (Me): Allows communication between Wickr Enterprise and Wickr Me. Is configured by the Super Administrator.
v5.62	Network Dashboard v2: The new administrative panel has been released in Enterprise. The new interface is more responsive and matches the Wickr Pro interface. Open Access License: Now controlled at the network level instead of per security group. Existing Security Group settings are inherited and unchanged after upgrading Enterprise. Apply the Open Access license in the Network Settings menu and have it available in any security group. The default is off.

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.

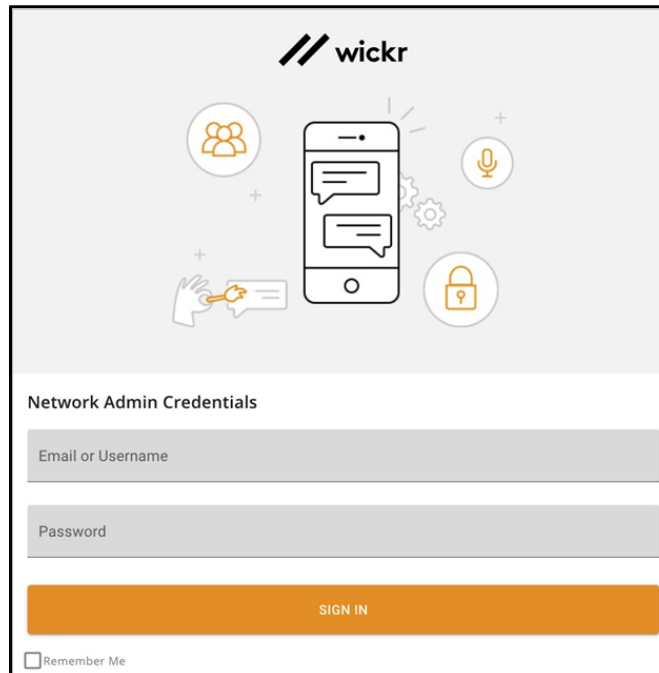
Super Administrator

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. 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 **SIGN IN** to log into the Super Administrator console.

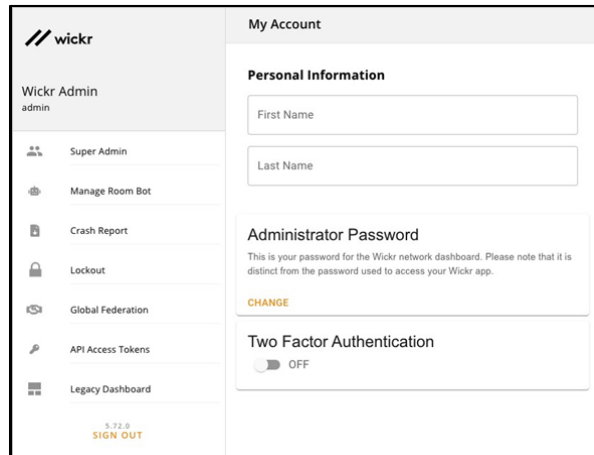


The image shows the Wickr Network Admin Credentials login form. At the top, the Wickr logo is displayed. Below the logo is a central graphic featuring a smartphone with speech bubbles, surrounded by icons for a group of people, a microphone, a hand holding a key, and a padlock. The form itself is titled "Network Admin Credentials" and contains two input fields: "Email or Username" and "Password". Below these fields is a large 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, they will be logged out of the original 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.

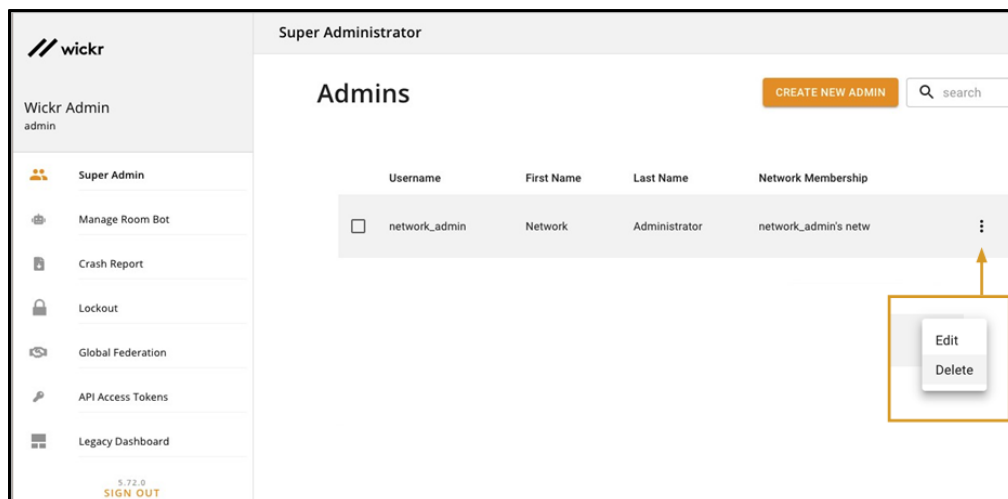


The screenshot shows the 'My Account' settings page in the Wickr Admin interface. On the left is a sidebar with the Wickr logo and a list of navigation items: 'Wickr Admin admin', 'Super Admin', 'Manage Room Bot', 'Crash Report', 'Lockout', 'Global Federation', 'API Access Tokens', and 'Legacy Dashboard'. The main content area is titled 'My Account' and contains three sections: 'Personal Information' with input fields for 'First Name' and 'Last Name'; 'Administrator Password' with a note about its distinctness from the app password and a 'CHANGE' button; and 'Two Factor Authentication' with a toggle switch currently set to 'OFF'. At the bottom of the sidebar, the version '5.72.0' and a 'SIGN OUT' link are visible.

Important! You cannot reset the Super Administrator account if the authentication method for 2FA is lost.

The available functions of the Super Administrator are:

- managing Network Administrators
- enabling or disable the Room Bot
- unlocking Network Administrators who have entered their password correctly
- managing Global Federation
- managing API keys with access to every network in the Enterprise deployment



The screenshot displays the 'Admins' management page for the Super Administrator. The sidebar is identical to the previous screenshot. The main content area is titled 'Admins' and includes 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 first name 'Network' and last name 'Administrator', belonging to 'network_admin's netw'. To the right of this row is a three-dot menu icon. A callout box with an arrow points to this menu, containing 'Edit' and 'Delete' options. The bottom of the sidebar shows the version '5.72.0' and a 'SIGN OUT' link.

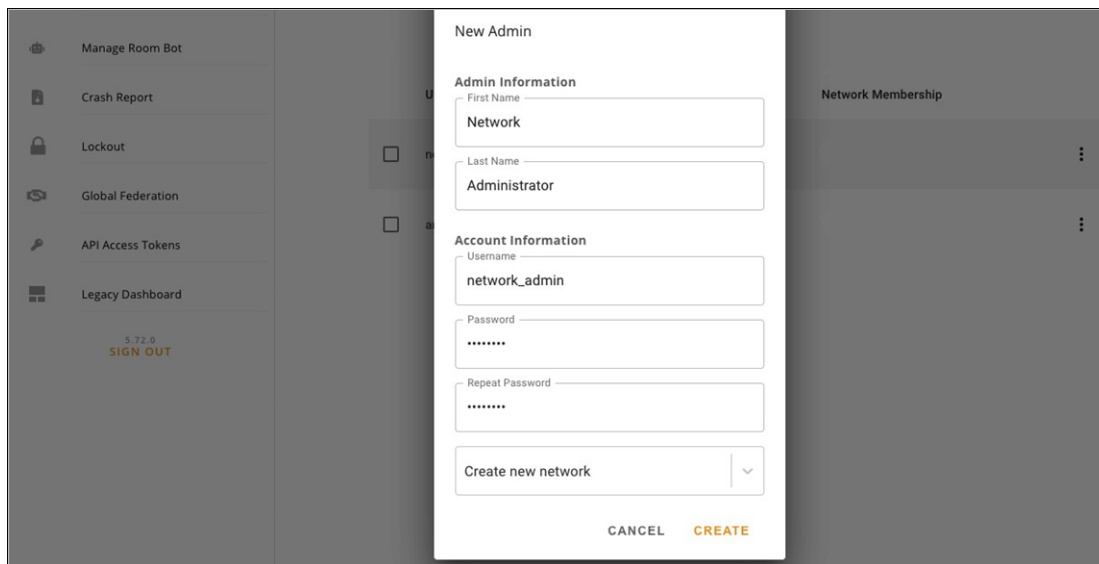
Creating a Network Administrator

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.

Important! We recommend at least two administrators per network. Having multiple administrators ensures the maximum coverage in case of emergencies.

- Network administrators can be added to an existing network using the network drop down or be assigned to a new network.
- Network administrator passwords can be updated at any time from this screen.
- Network administrators can be deleted from this screen.

To create a network administrator, fill in their username and password. First and last name are *optional*.

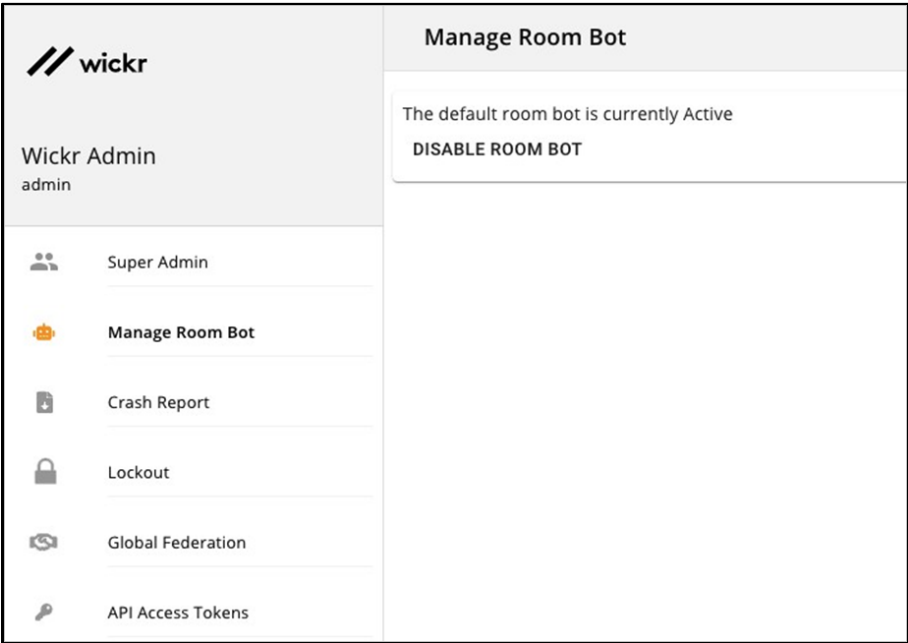


The screenshot shows a 'New Admin' modal form. On the left is a sidebar with navigation links: 'Manage Room Bot', 'Crash Report', 'Lockout', 'Global Federation', 'API Access Tokens', and 'Legacy Dashboard'. At the bottom of the sidebar is a version indicator '5.72.0' and a 'SIGN OUT' button. The modal form itself has two main sections: 'Admin Information' and 'Account Information'. Under 'Admin Information', there are fields for 'First Name' (containing 'Network') and 'Last Name' (containing 'Administrator'). Under 'Account Information', there are fields for 'Username' (containing 'network_admin'), 'Password' (masked with dots), and 'Repeat Password' (also masked with dots). At the bottom of the form is a dropdown menu labeled 'Create new network' with a downward arrow. At the very bottom of the modal are two buttons: 'CANCEL' and 'CREATE'.

Manage the Room Bot

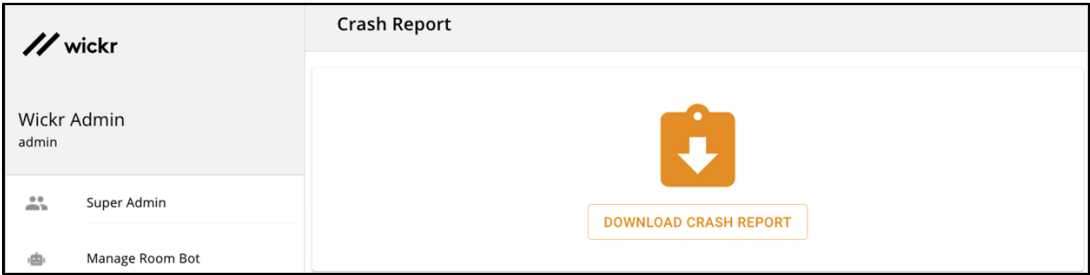
The Room Bot allows Network Administrators to deploy pre-created rooms managed by this bot. The bot will add all users in a particular Security Group or Network to a room and automatically re-add users if they attempt to leave. Multiple rooms can be created for any group.

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



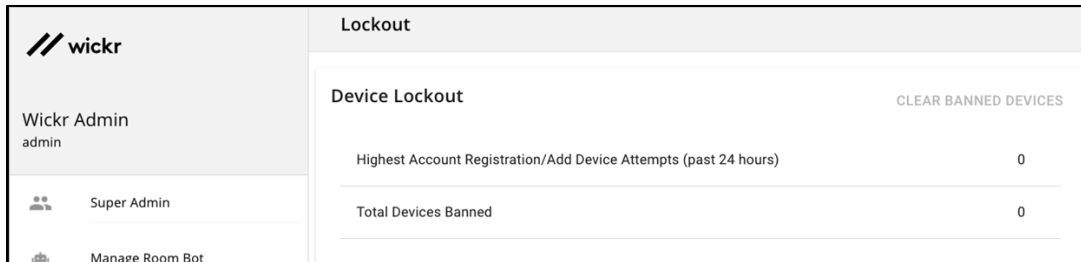
Crash reports

Super Administrators can also generate Crash Reports in case of failures. Provide the report to Wickr in the event of failures, however, note that these files and more are available server-side and replicated.



Registration and Administrator Lockout

Super Administrators can unlock Network administrator accounts 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.

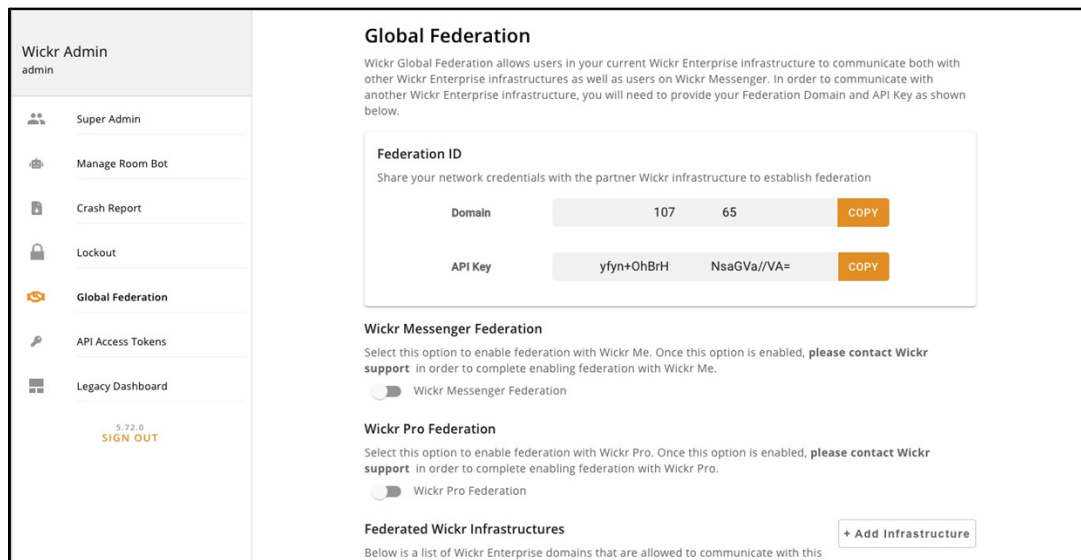


Manage Global Federation

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, contact Wickr Support to whitelist your deployment.
- For Global federation, see the Global Federation: Setup and Configuration Guide.



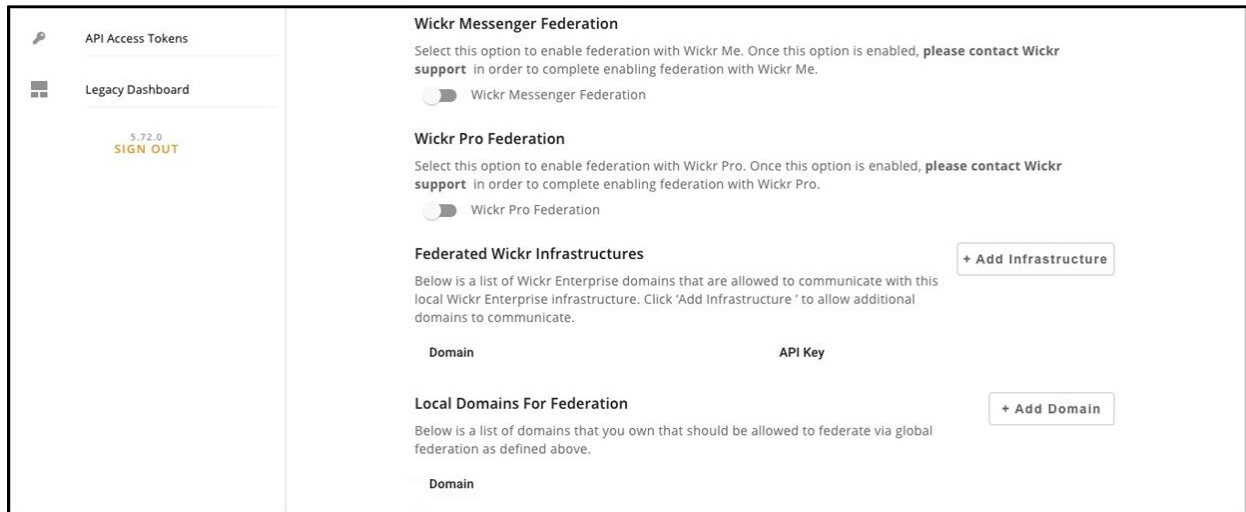
Global Federation requires domain names and a new username style to be used.

- **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.

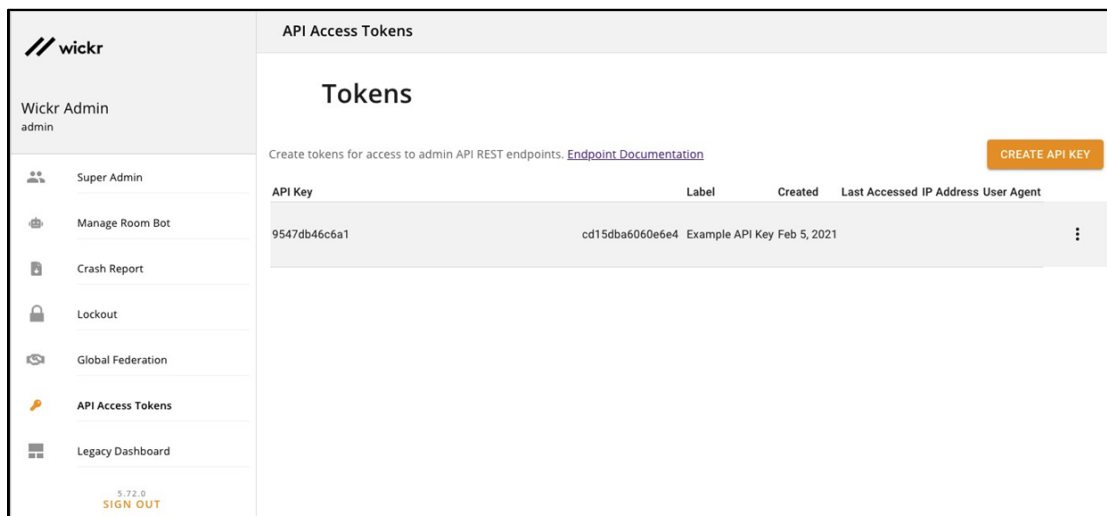
For example, if the domain “example.com” and “testing.com” were added here, the following users would be valid:

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



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.

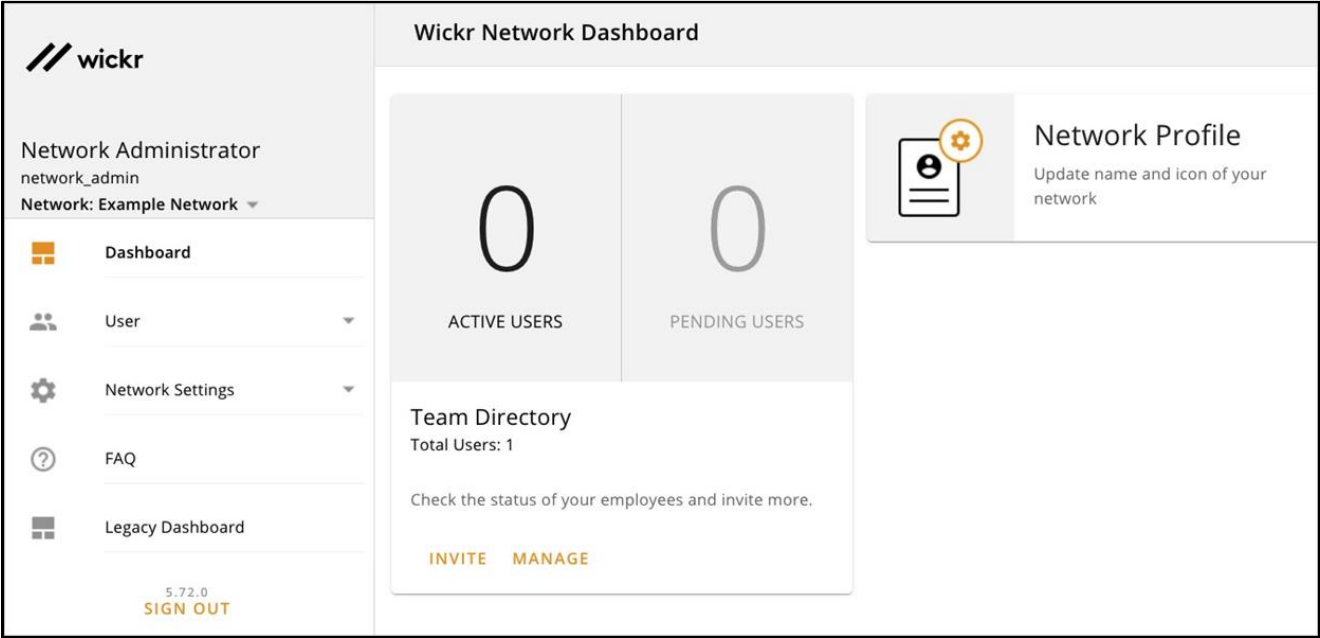


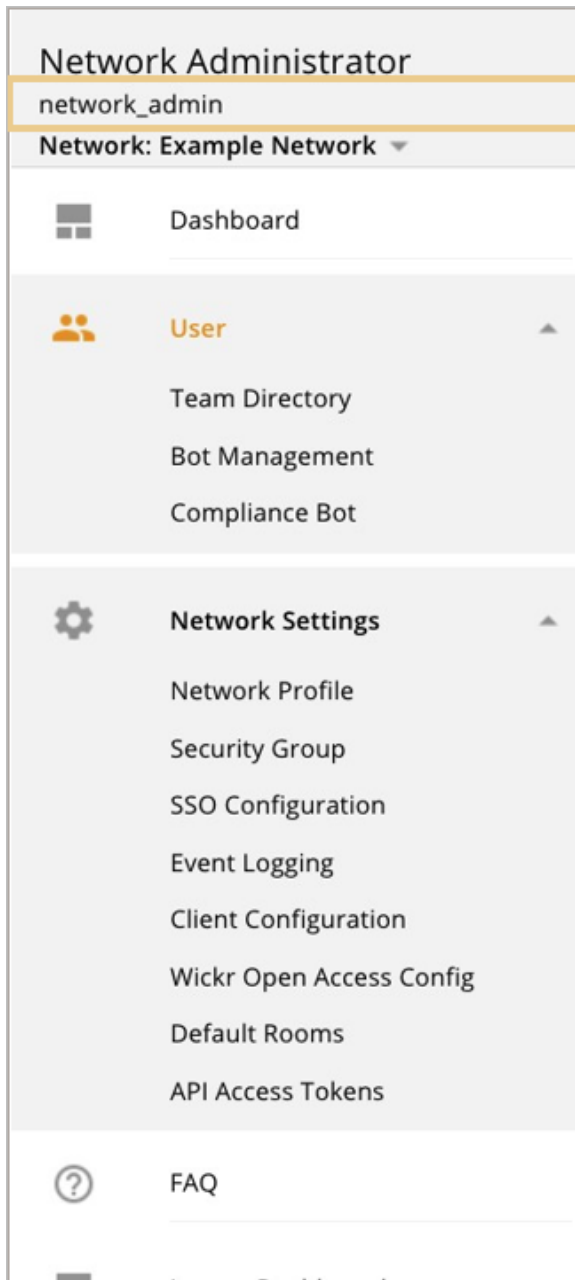
Network Administrator

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.

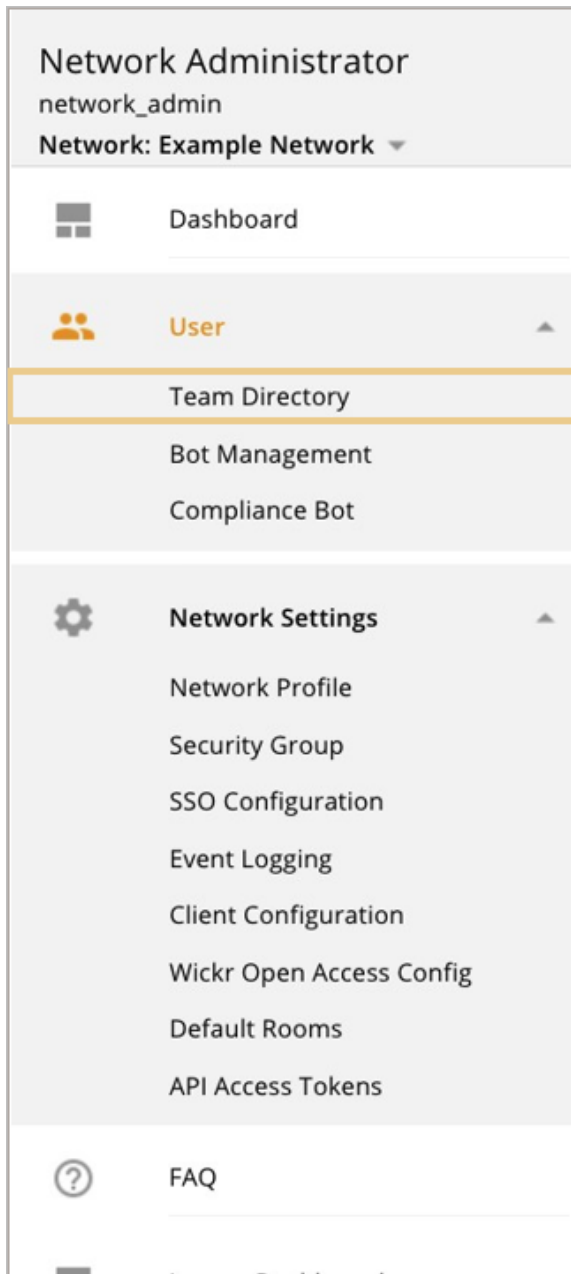




Account Settings

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.

A screenshot of the 'My Account' settings page. The page has a light gray header with the title 'My Account'. Below the header, there are three main sections. The first section is 'Personal Information', which contains two text input fields: 'First Name' with the value 'Network' and 'Last Name' with the value 'Administrator'. The second section is 'Administrator Password', which includes a note: 'This is your password for the Wickr network dashboard. Please note that it is distinct from the password used to access your Wickr app.' and a 'CHANGE' button. The third section is 'Two Factor Authentication', which features a toggle switch currently set to 'OFF'.



Team Directory

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

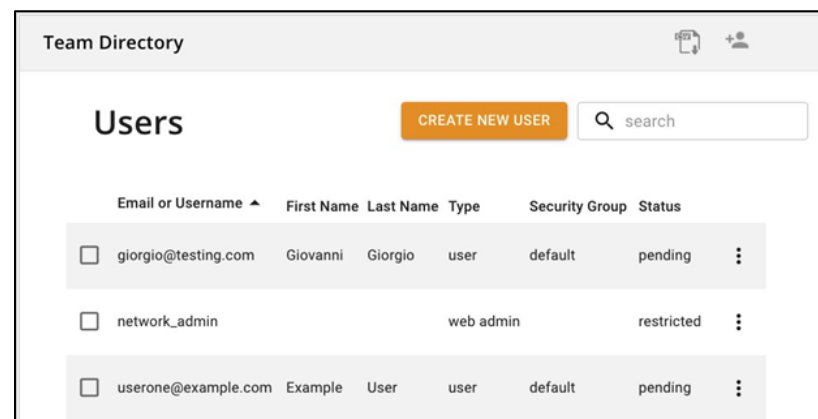
User statuses can be:

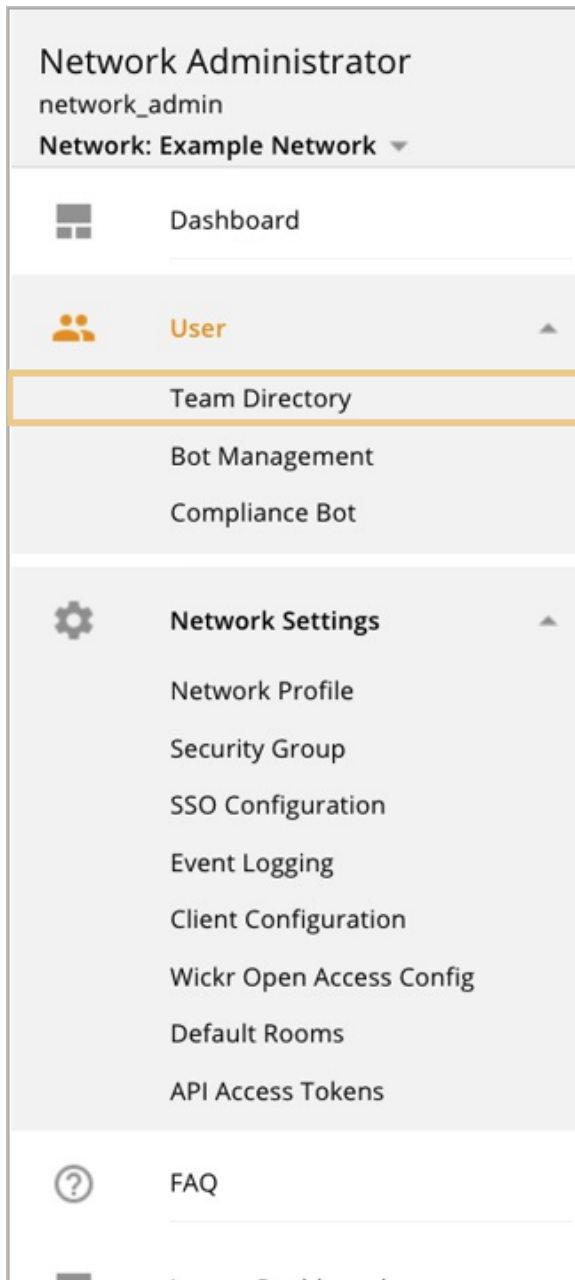
- **Pending:** The user has not registered.
- **Active:** The user has registered and is able to receive messages.
- **Suspended:** The user is unable to sign in to their account, but still active.
- **Restricted:** This notes that the user cannot use Global Federation or is strictly an Administrator.

Note: 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.





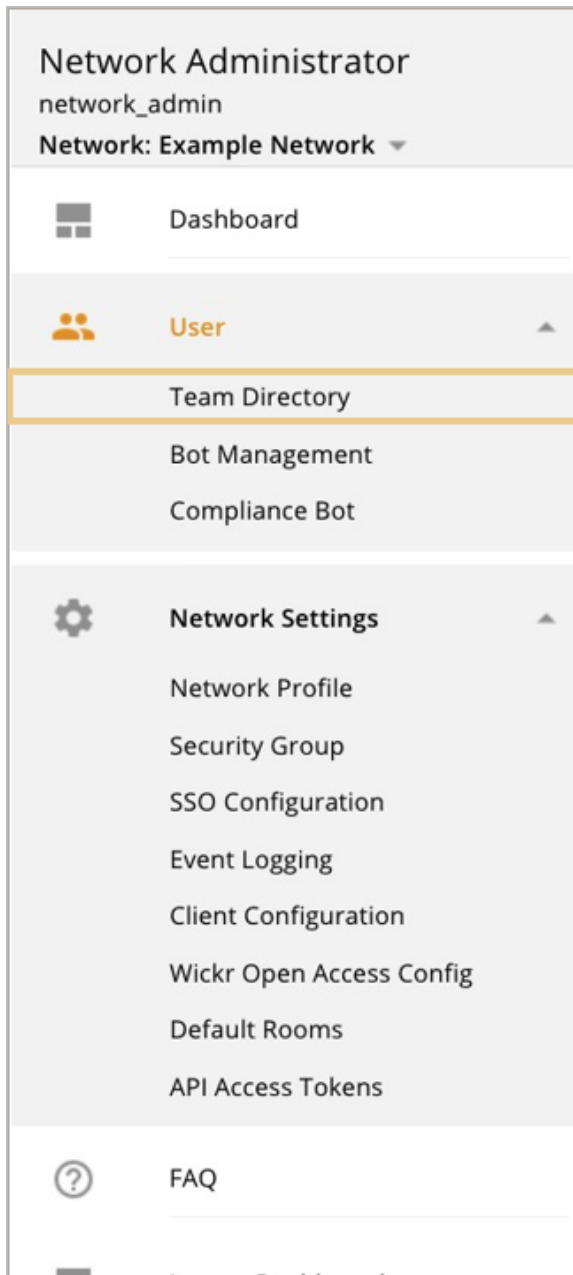
Creating a user manually requires the following information:

- 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

A screenshot of the 'New User' form in the Network Administrator interface. The form is a modal dialog with a white background and a grey border. It contains two main sections: 'User Information' and 'Account Information'. The 'User Information' section has fields for 'First Name' (filled with 'Giovanni') and 'Last Name' (filled with 'Giorgio'). The 'Account Information' section has fields for 'Email or Username' (filled with 'giorgio@testing.com'), 'Password' (masked with dots), and 'Repeat Password' (masked with dots). Below these is a dropdown menu for 'Security Group' (currently set to 'default') and a checkbox for 'Grant admin privileges' (unchecked). At the bottom right are 'CANCEL' and 'CREATE' buttons. The background shows a blurred view of the administrator interface with a 'NEW USER' button and a search bar.



Inviting Administrators

Network Administrators can add an 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.

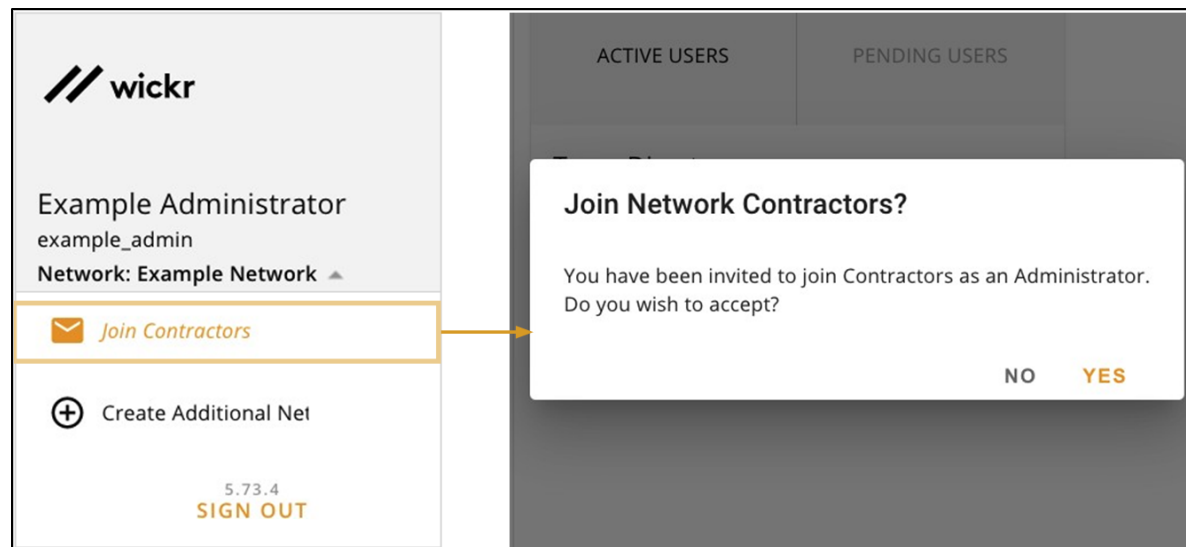
To add an Administrator:

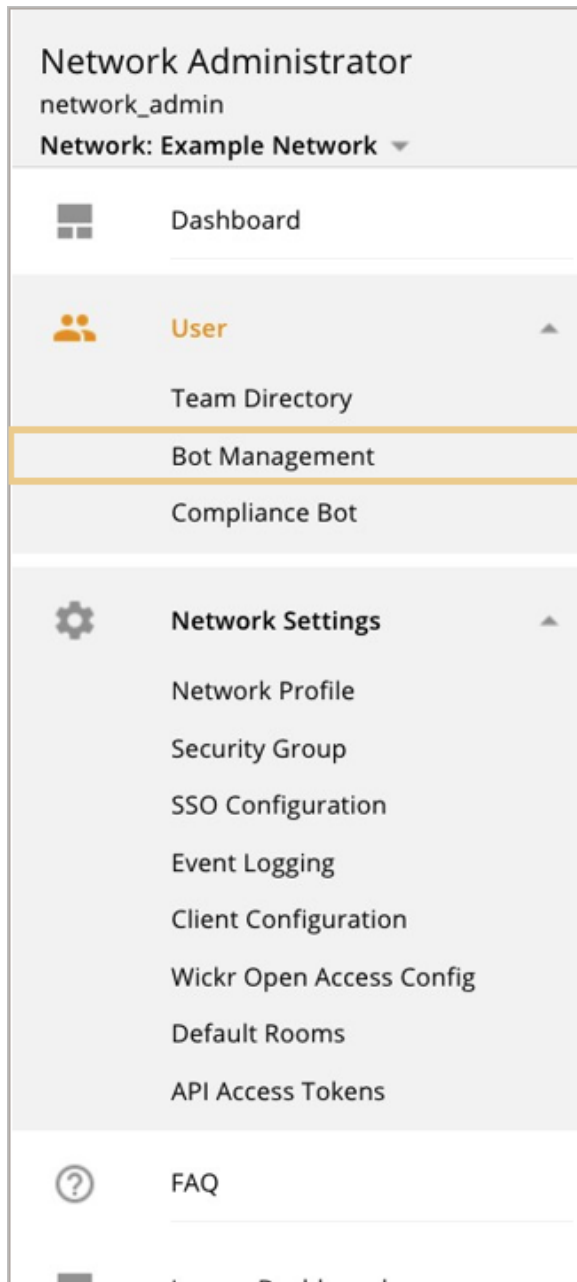
1. Click the **Create User** button.
2. Enter the username of the other admin in the **Username** field and select the **Grant Admin Privileges** checkbox.
3. Click **Create** to invite the admin to your network. For example:

A screenshot of the 'Create User' form in the Network Administrator interface. The form is titled 'User Information' and 'Account Information'. It includes fields for 'First Name', 'Last Name', 'Username' (with the example 'example_admin'), 'Password', and 'Repeat Password'. There is a dropdown menu for 'default' and a checkbox labeled 'Grant admin privileges' which is checked. At the bottom right, there are 'CANCEL' and 'CREATE' buttons. The background shows a blurred view of the Network Administrator sidebar menu.

Accepting Network Invites

Network Administrators can view their invites in the **Network** drop-down on the upper left of the page. Clicking the “Join [Network Name]” option will ask the user to confirm.



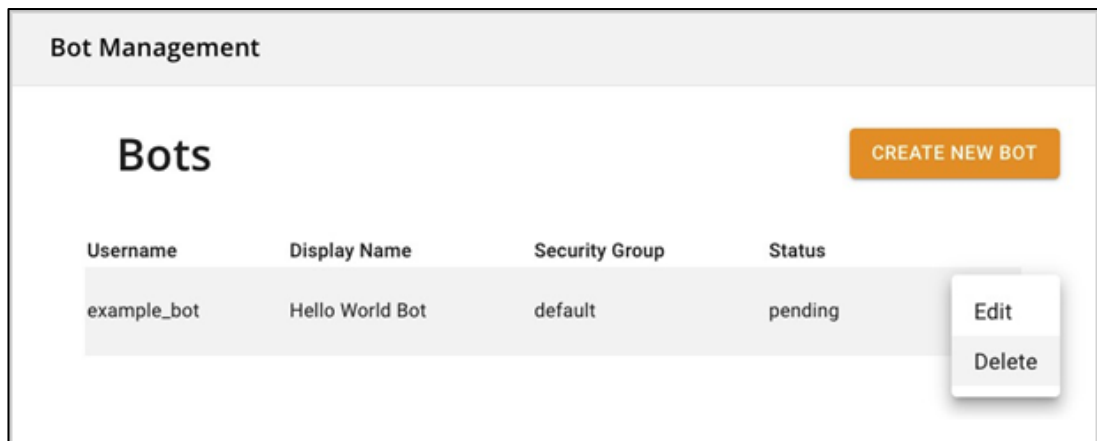


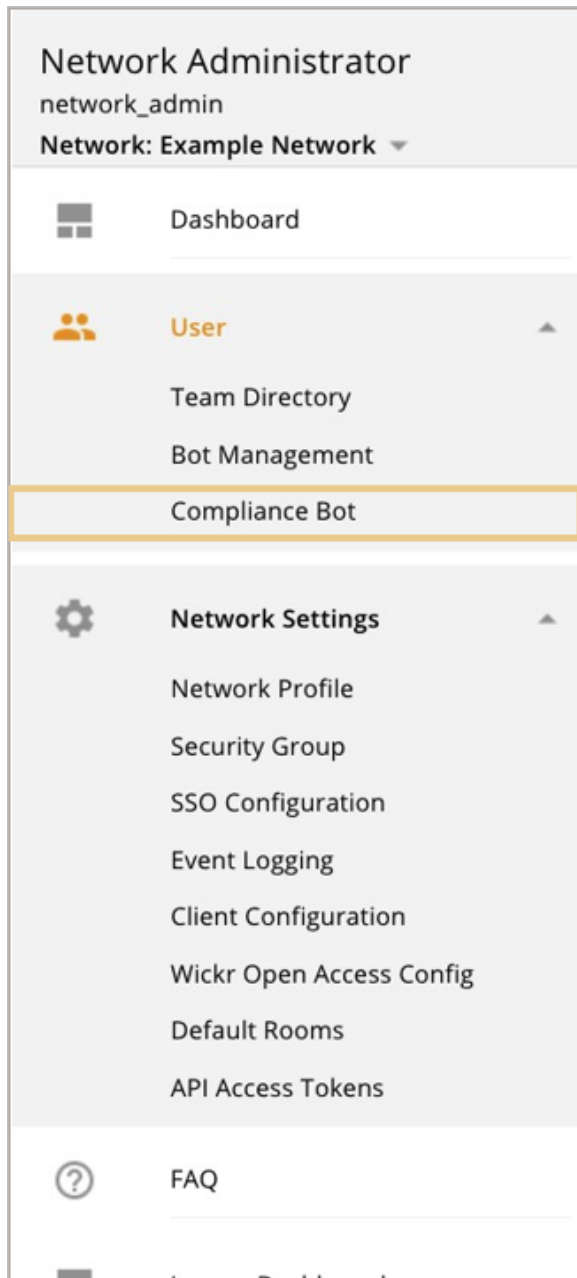
Bot Management

From this screen an administrator can:

- Create a bot
- Delete a bot
- Edit the information of a Pending bot Usernames must end with “bot”.

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





Compliance Bot

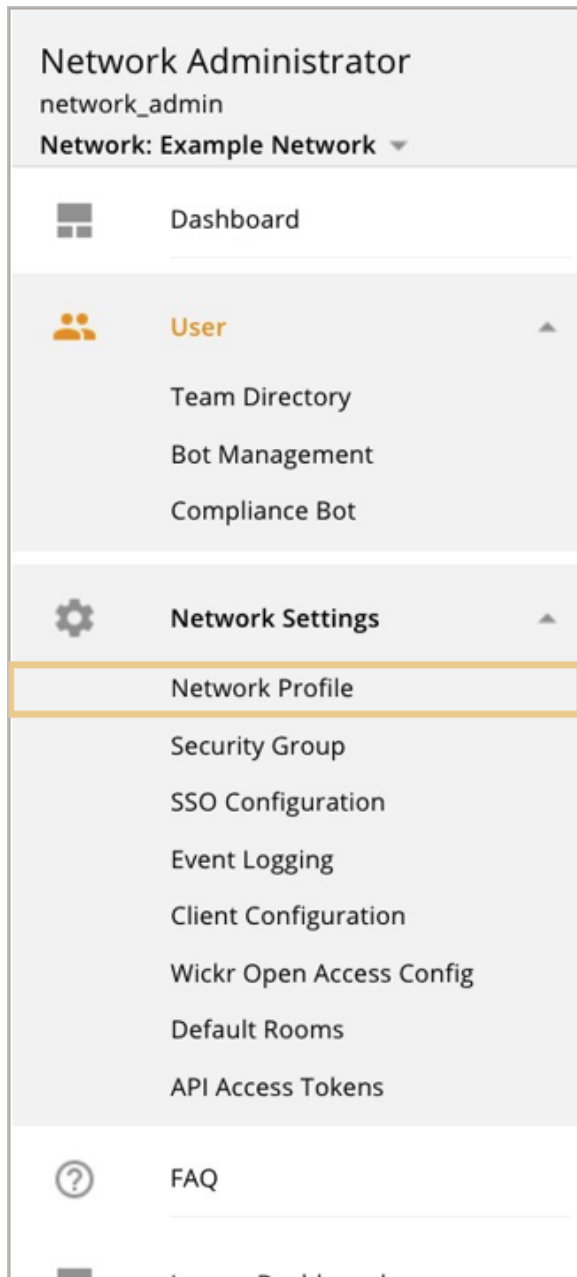
The Compliance bot is an additional service only available within Wickr Enterprise.

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 *Compliance Service Deployment Guide*.

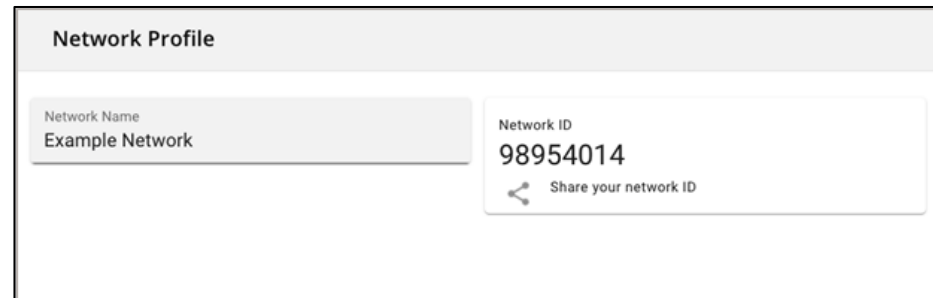
The image shows a screenshot of the 'Compliance Bot Setup' form. The form has a title 'Setup' and a descriptive text: 'To create your compliance bot, you will need to set up a username and initial password. Once created, the bot will be inactive until the Docker image is started & configured.' Below this text are two input fields. The first field is labeled 'compliance_bot' and contains the text 'compliance_bot'. The second field is a password field, indicated by six dots, and is currently empty. At the bottom right of the form is an orange 'SUBMIT' button.

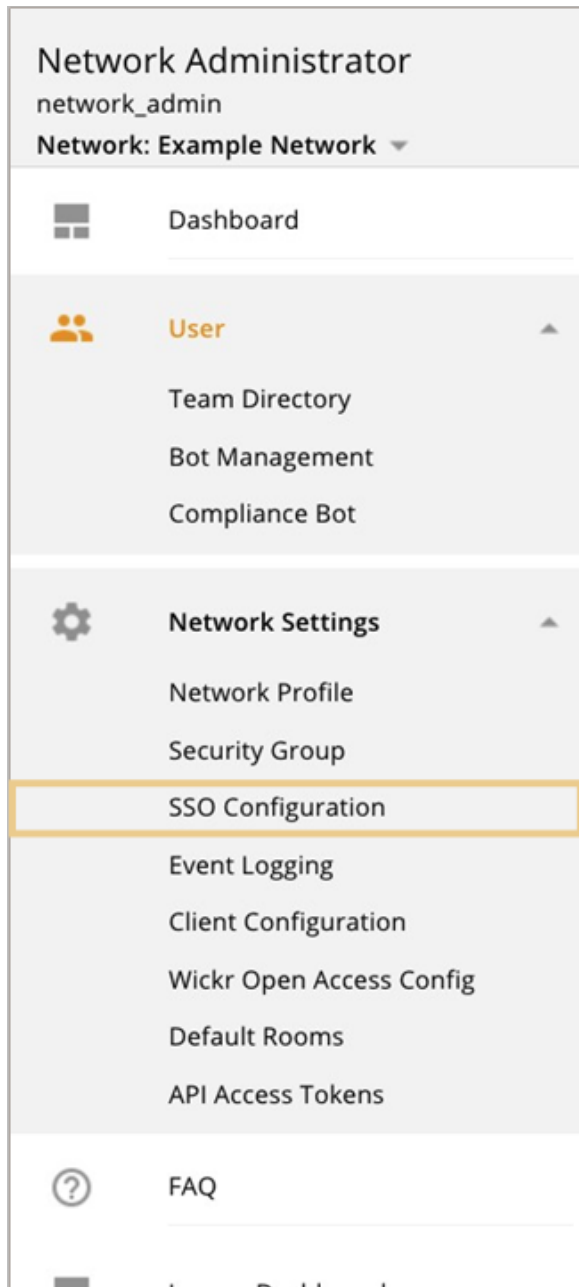


Network Profile

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.





SSO Configuration

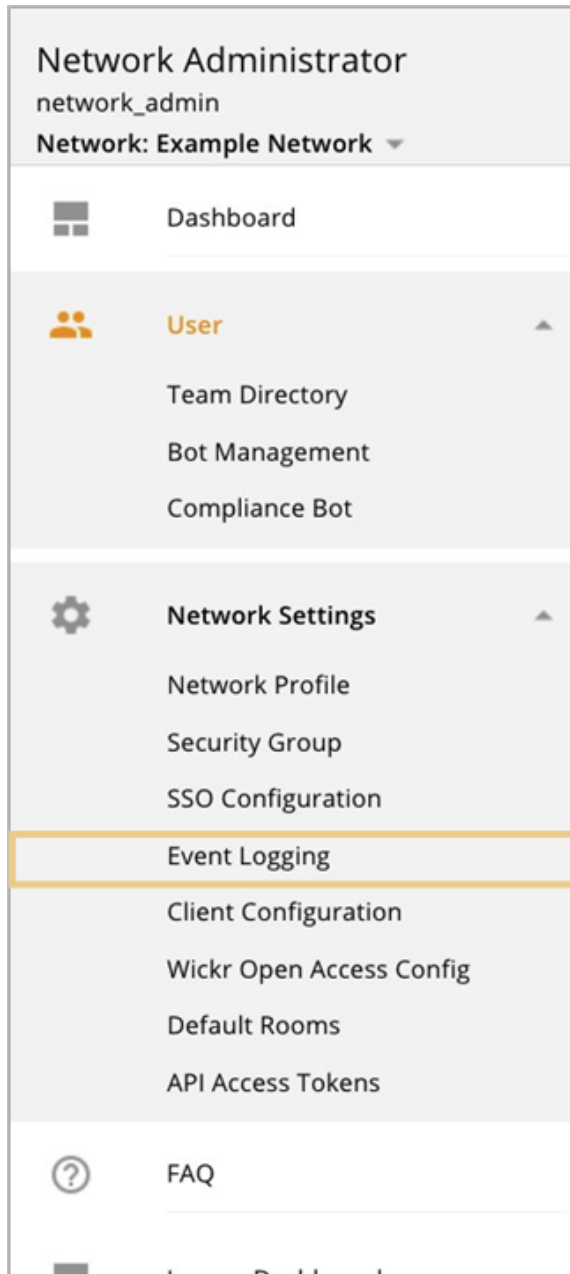
The SSO Configuration page allows an Administrator to add SSO authentication to a specific network. If using ADFS it is also possible to sync Wickr Security Groups with Active Directory user Groups.

- **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.

Note: 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.

A screenshot of the 'Single Sign-on & LDAP Configuration' page. It has three main sections: 1. 'Network Endpoint' with a description 'Wickr endpoint to use on your SSO IDP side to connect to Wickr.' and a 'Redirect URI' field containing 'https://107. .65/deeplink/oidc.php' with a 'COPY' button. 2. 'SSO Configuration' with a description 'SSO provider connection details' and a 'START' button. 3. 'Security Group Synchronization' with a description 'Works best with ADFS 4.0+ on Windows Server 2016 or newer.' and a 'SETUP' button.

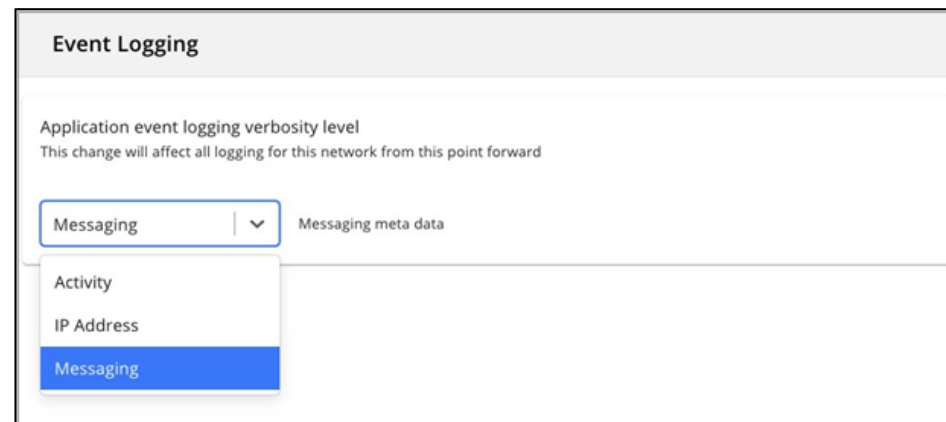


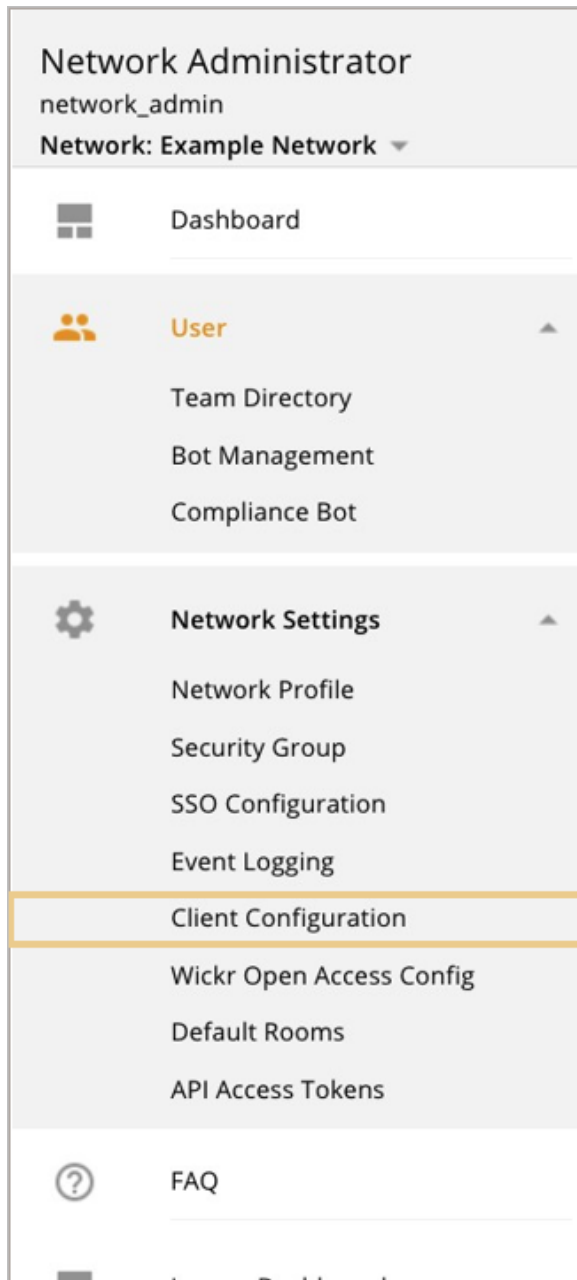
Event Logging

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.





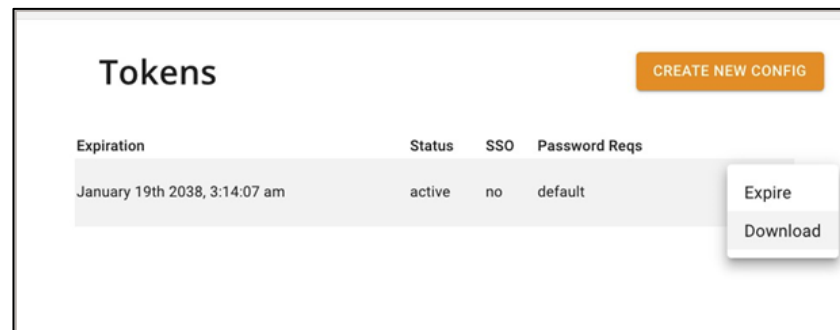
Client Configuration

Config file or deeplinks created on the **Client Configuration** screen are the second most important thing an end user needs to successfully register and use Wickr Enterprise.

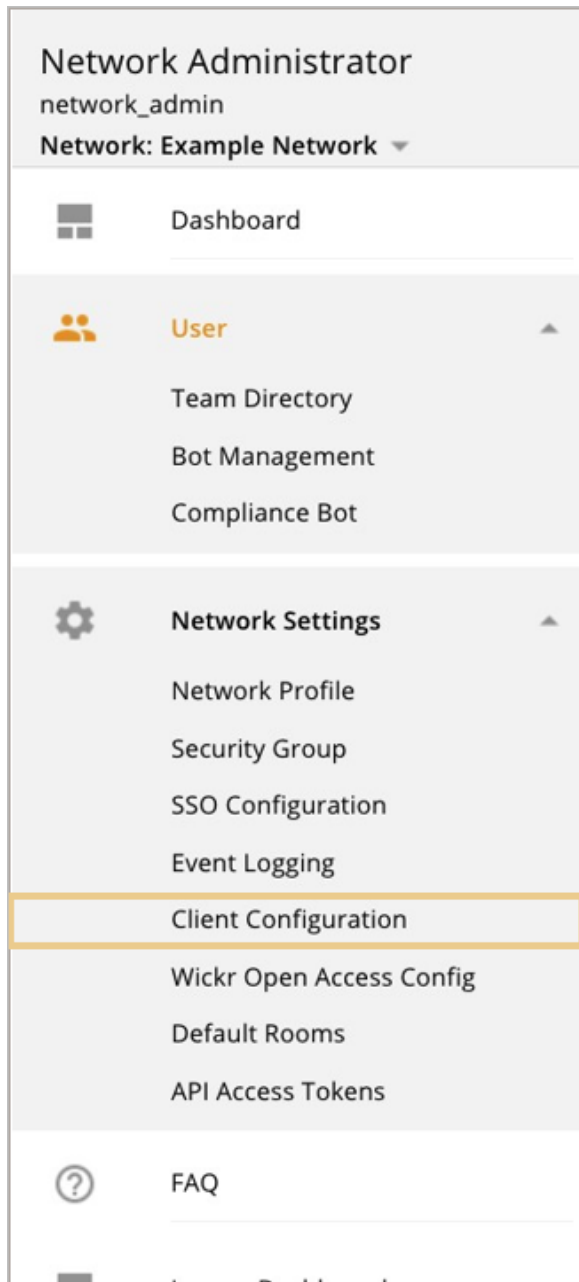
Note: Deeplink passwords are *optional*.

It displays currently active files or deeplinks, and will allow the Administrator to expire an active token, as well as download it again.

Note: It is not possible to download configuration files created before version 5.70.



The files and links are only used for the initial connection to Enterprise Config files and must be password protected, as the information within is encrypted.

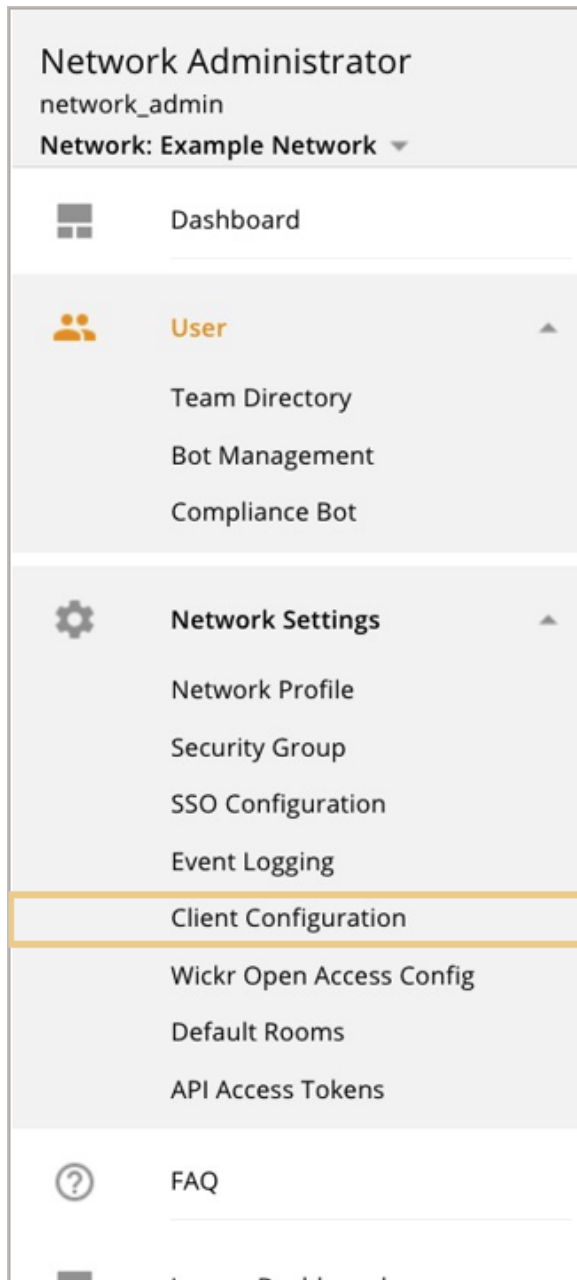


This allows the client to establish a connection to the Enterprise service, but a user must still have a valid username and password to complete the Registration or Sign In process.

The image shows a 'Client Configuration Files' dialog box with a 'Create Configuration File' form. The form includes a 'Security Group' dropdown menu set to 'default', an 'Expiration Period' dropdown menu set to '30 days', a 'Password' field (masked with dots, with a note 'maximum 128 characters'), and a 'Repeat Password' field (also masked). Below these fields are two toggle switches: 'Generate auto configuration deeplink' (which is turned on) and 'Password protect deeplink' (which is turned off). A note explains the deeplink: 'Create a link that will take users to their installed Wickr Enterprise app when clicked and automatically install this configuration, no file required.' Another note for the password toggle says 'Require users to provide the password entered above when using the deeplink.' At the bottom right are 'CANCEL' and 'CREATE' buttons. On the left side of the dialog, a partial sidebar menu is visible with items like 'Administrator', 'Network', 'ard', 'k Settings', 'k Profile', 'r Group', 'nfiguration', 'ogging', 'onfiguration', 'pen Access Config', 'Rooms', 'ess Tokens', 'Dashboard', and '5.72.0 GN OUT'.

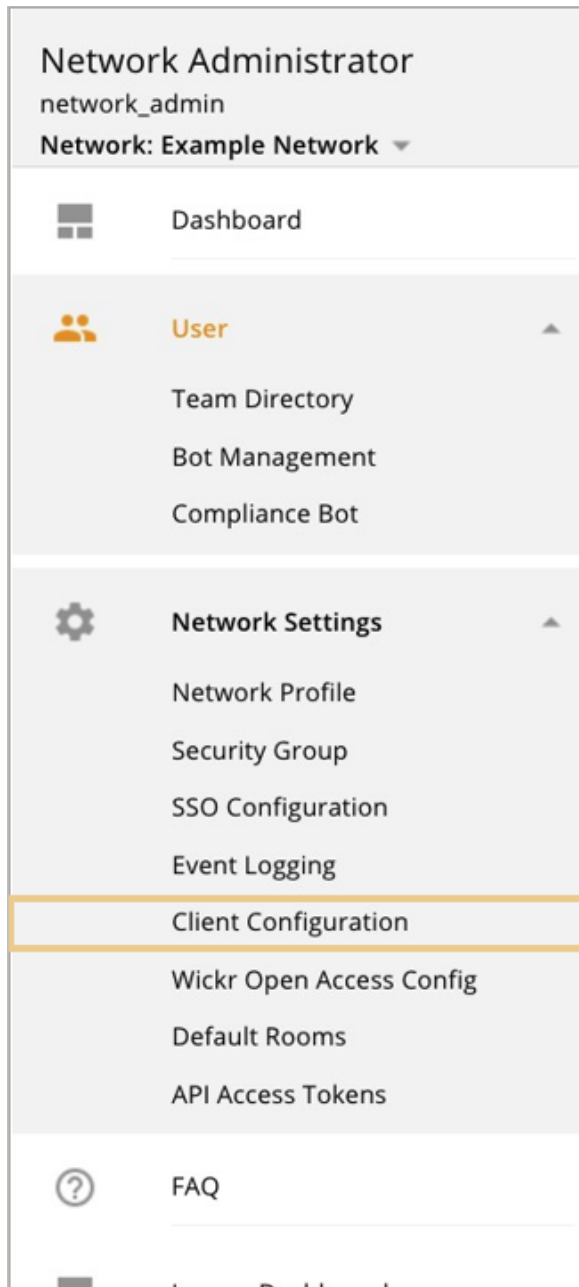
After creating the configuration file, a Deeplink URL and a Deeplink Landing Page URL will also be created.

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.



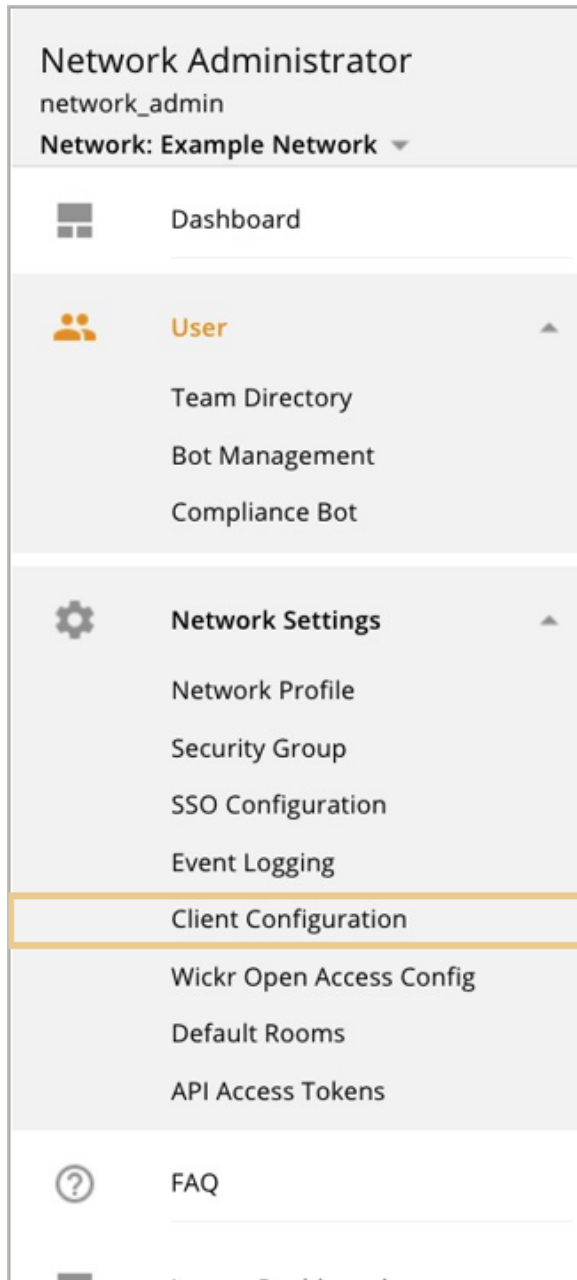


Certificate Pinning

Certificate pinning is an online application security technique that accepts only authorized pinned certificates for authentication of client-server connections. With certificate pinning, the SSL certificate is hard-coded into application code. When the application communicates with the server, it checks whether the same certificate is present.

- If certificate pinning is enabled, Wickr clients will ONLY trust and connect to Enterprise service hosts that present the specified certificate(s).
- If certificate pinning is disabled, Wickr clients will use the standard, platform-based certificate validation when connecting to their Enterprise host.

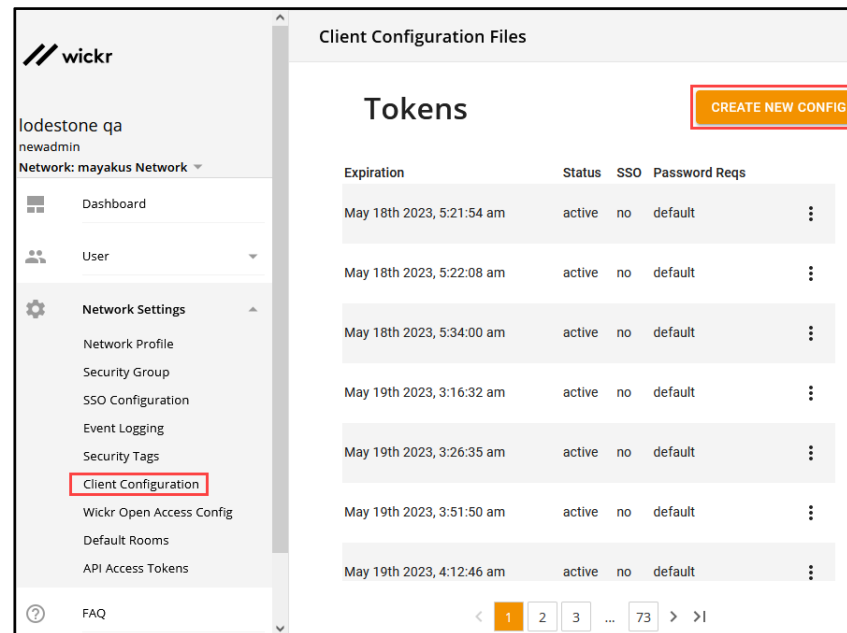
Note: Client platforms can vary in what they consider to be valid [X.509 certificates](#). If you plan on using a private certificate, (i.e., certificates not obtained from a Digital Certificate Authority), we strongly recommend that you enable certificate pinning to ensure that your certificate is trusted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



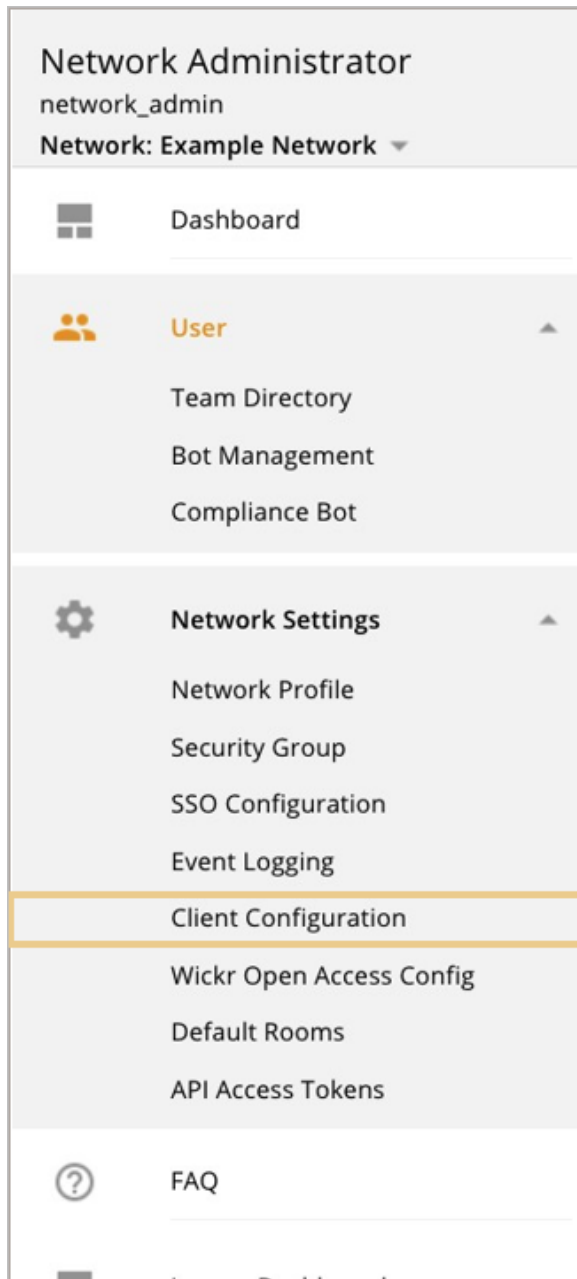
Enabling certificate pinning

To enable certificate pinning:

1. On the Wickr Admin Console, choose **Network Settings > Client Configuration**, and then click **CREATE NEW CONFIG**.

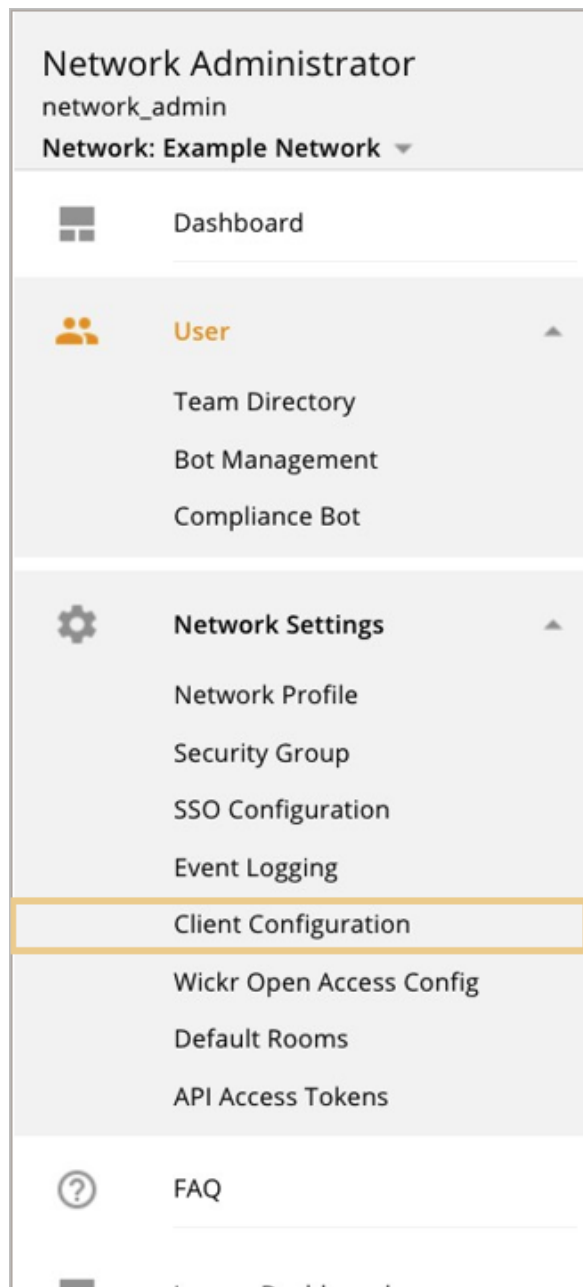


2. On the **Create Configuration File** window, follow these steps:
 - a. Choose a security group from the **Security group** drop-down list.
 - b. Choose the expiration period from the **Expiration period** drop-down list.
 - c. Enter a password into the **Password** and **Repeat password** fields.

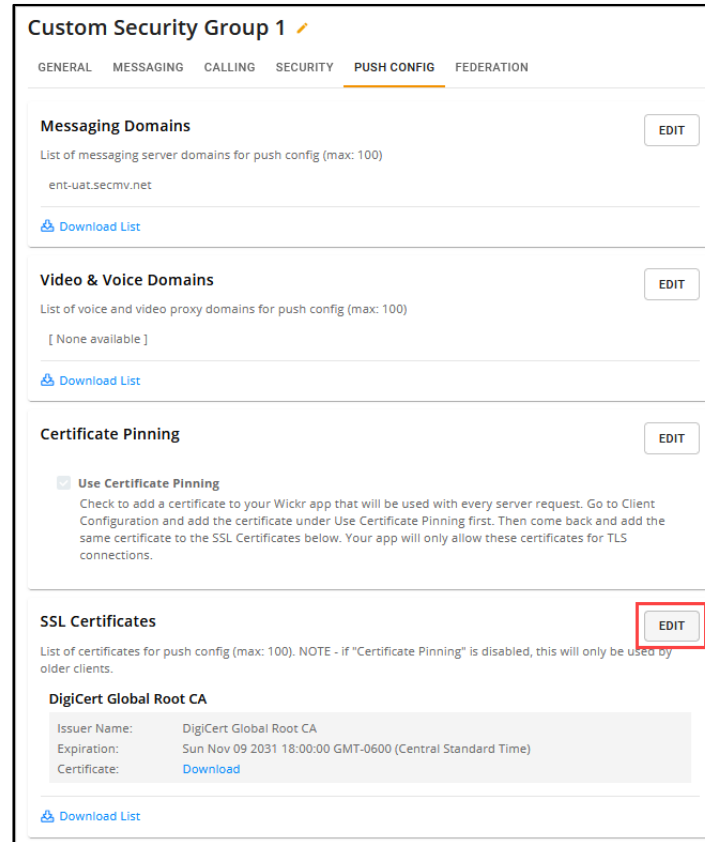


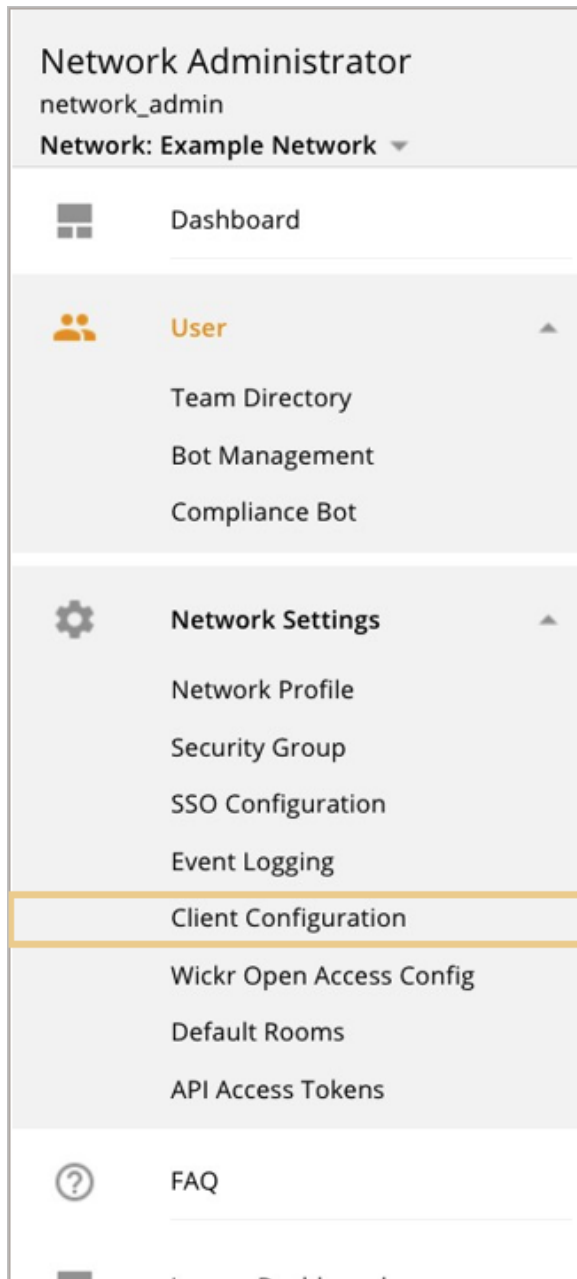
- d. *Optionally*, toggle **Generate auto configuration deeplink** to generate an auto configuration deep link to take users to their installed Wickr Enterprise app when clicked.

A screenshot of the 'Create Configuration File' form. It includes a 'Permission source' dropdown set to 'Custom Security Group 1' with a note 'open access disabled'. The 'Expiration Period' is set to '30 days'. There are fields for 'Password' and 'Repeat Password', both masked with dots. At the bottom, there is a checkbox labeled 'Generate auto configuration deeplink' with a description: 'Create a link that will take users to their installed Wickr Enterprise app when clicked and automatically install this configuration, no file required.'

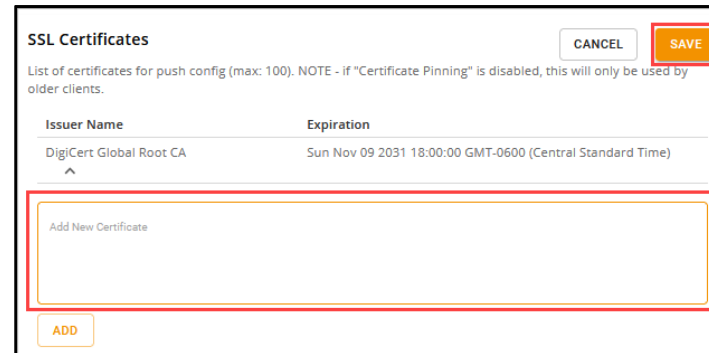


- f. Enter the **FQDN** or **IP address** of the server where your Wickr instance is hosted in the **Service host** field.
 - g. Select the **Use certificate pinning** option to add a certificate to your Wickr app that will be used with every server request to turn Certificate Pinning on.
 - h. Under **SSL certificate**, copy the contents of the SSL certificate.
 3. Paste the contents of the SSL certificate in the load config file.
 - a. On the Wickr Admin Console, choose **Network Settings > Security group**, then click **DETAILS** for the security group you want to disable certificate pinning.
 - b. Select the **PUSH CONFIG** tab, then click **EDIT** under the **SSL Certificates** section.

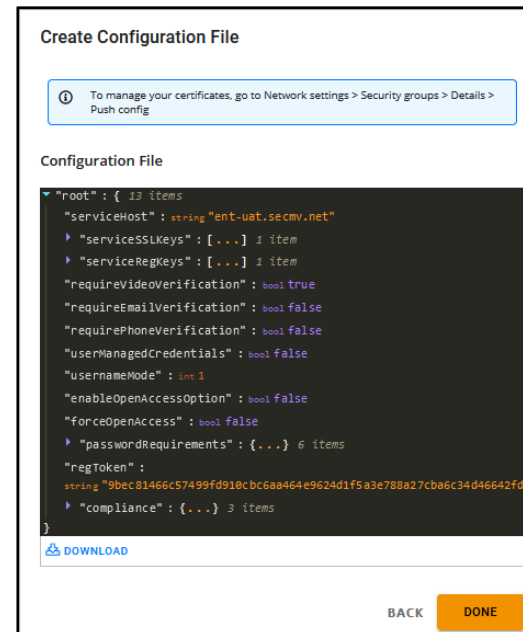


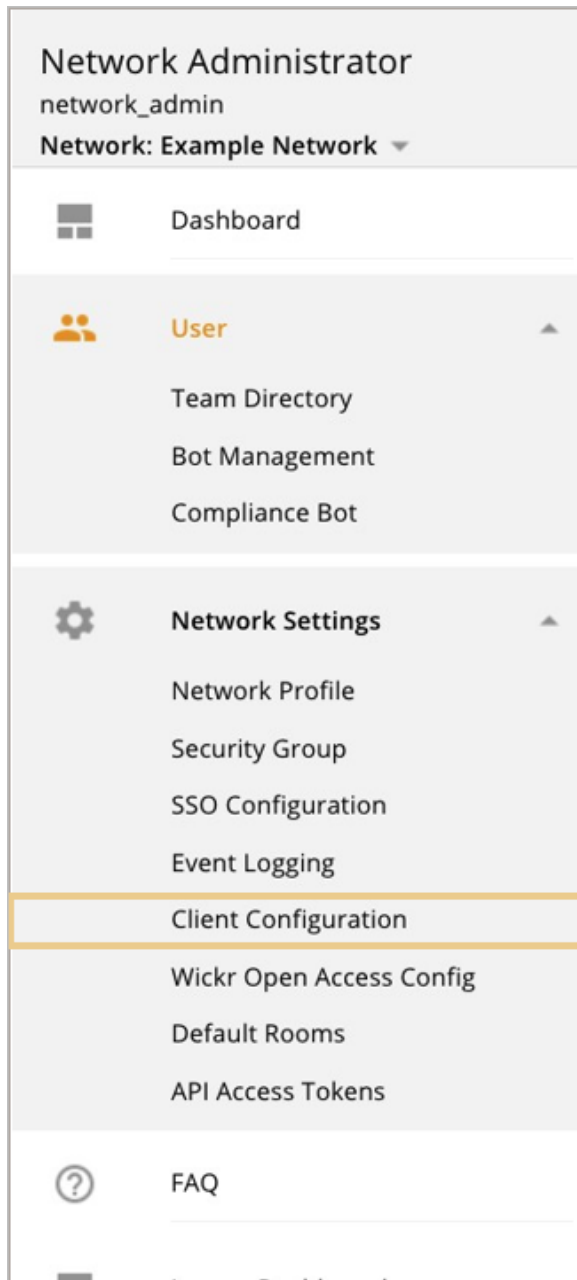


- c. Paste the contents of the SSL certificate in the **Add New Certificate** field, then click **SAVE**.



- d. *Optionally*, click **ADD** to add multiple certificates.
4. On the **Create Configuration File** window, click **CREATE**.
5. On the **Create Configuration File** pop-up window, click **DONE**.





Migration to disable certificate pinning

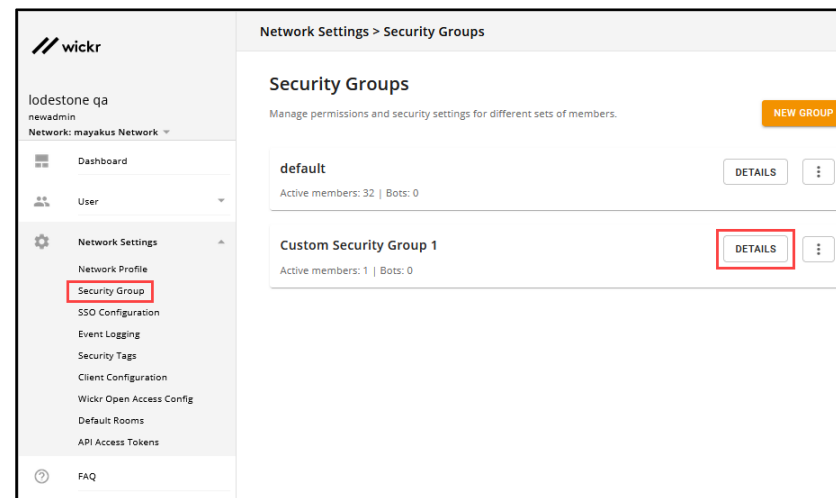
Important! Do not disable certificate pinning if you are using a self-signed certificate.

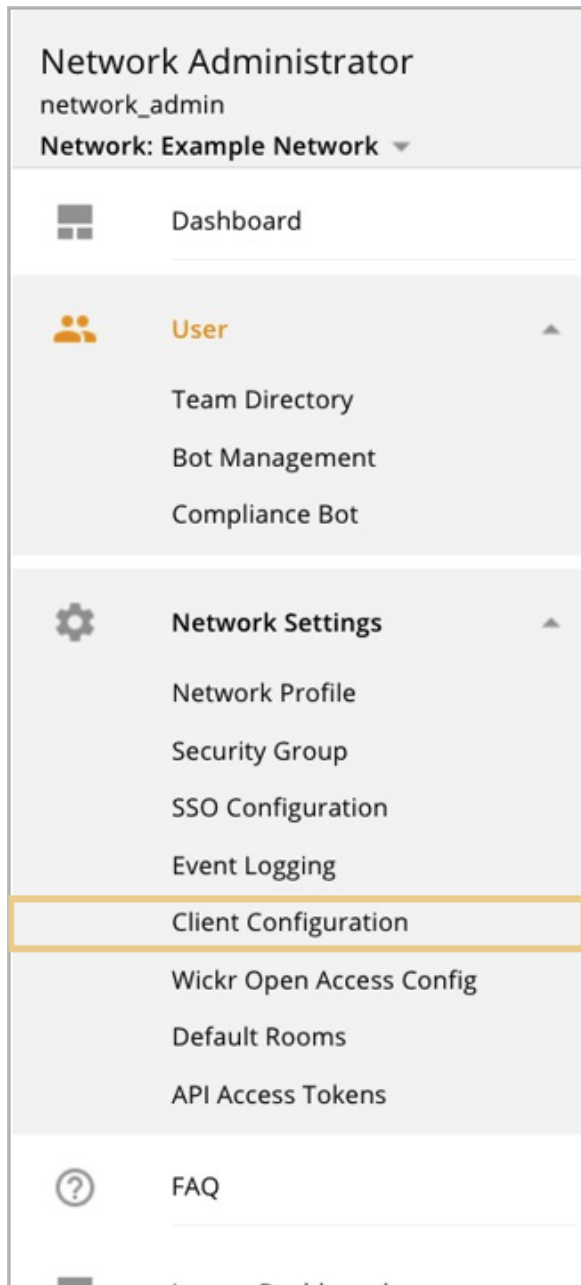
You may want to disable certificate pinning to avoid losing the ability to respond to certificate issues. For example, if the certificates are rotated on a regular basis, the application needs to also be updated regularly. During certificate rotation, the current certificate expires and a new certificate must be regenerated, if you have certificate pinning enabled.

When a new certificate is generated and pushed down to all clients/devices using the **Push config** option, only the active clients/devices can get the updated certificate. If you have devices that are not active (switched off or app killed), they won't get the updated new certificates. Later, when they become available, the devices won't receive the push config, which leads to a bad state for your Wickr app (expired certificates). The only way to reactivate the Wickr app is by resetting the app, which can be avoided if you disable certificate pinning.

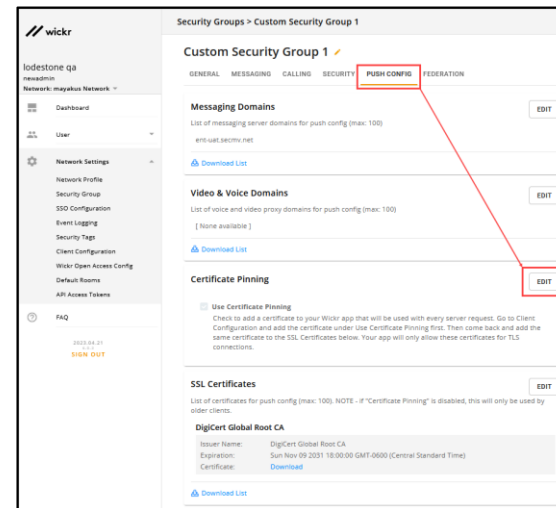
To disable certificate pinning:

1. In the Wickr Admin Console, choose **Network Settings > Security Group**, then click **DETAILS** for the security group.

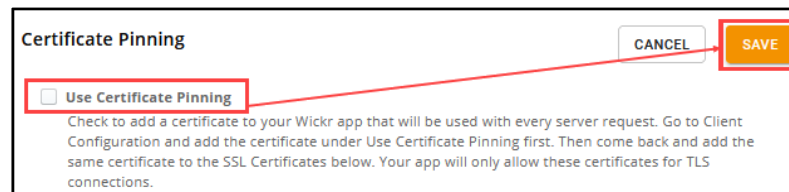


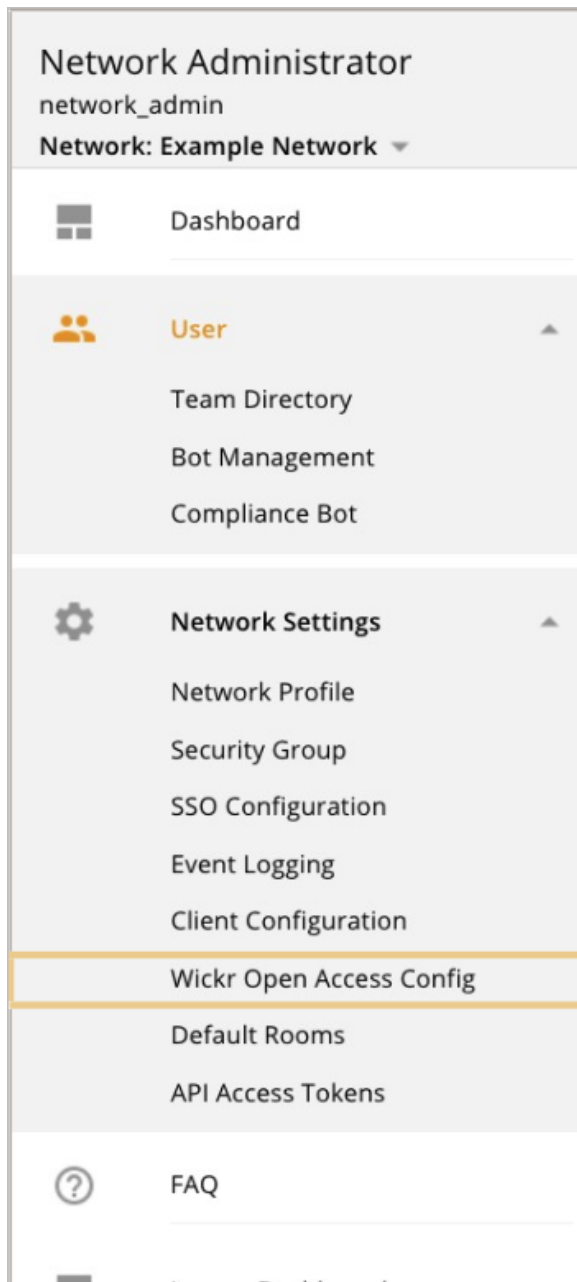


- On the selected security group page, select the **PUSH CONFIG** tab, then click **EDIT** in the **Certificate Pinning** section.



- Deselect **Use Certificate Pinning**, then click **SAVE**.



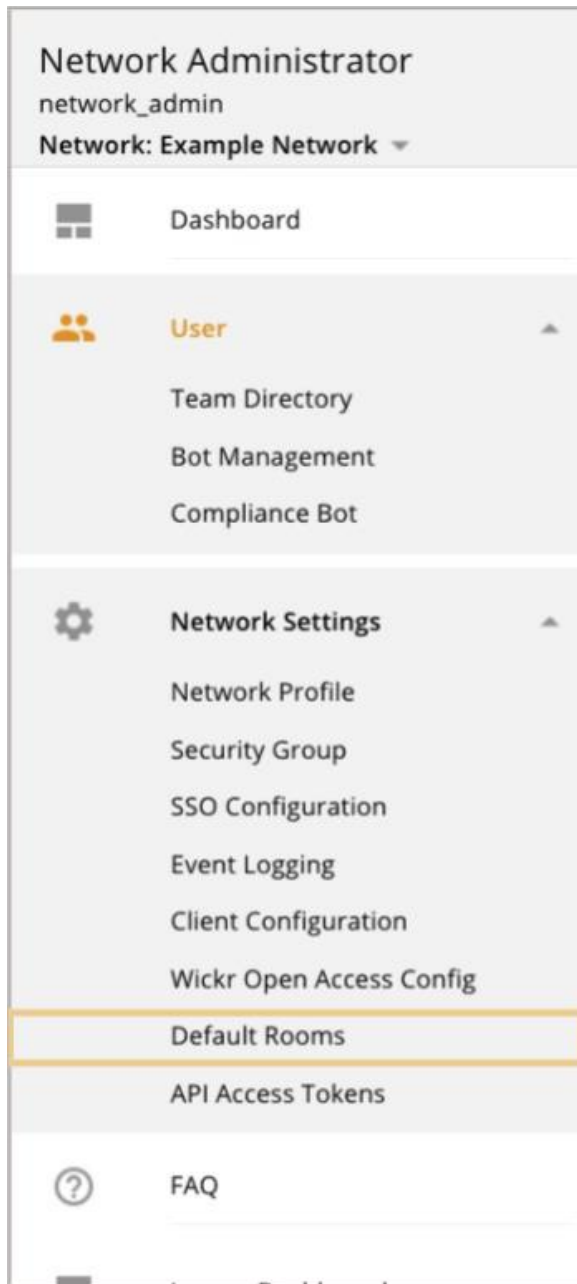


Wickr Open Access Config

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 to **ON** for every user in a security group.

A screenshot of the 'Wickr Open Access Configuration' page. The page has a title bar 'Wickr Open Access Configuration'. Below it, the section 'Wickr Open Access' is shown with 'SAVE' and 'CLEAR' buttons. A message states: 'In order to use Wickr Open Access, you must enter your configuration license below.' Below this message is a large, empty text input field labeled 'Configuration License'.



Default Rooms

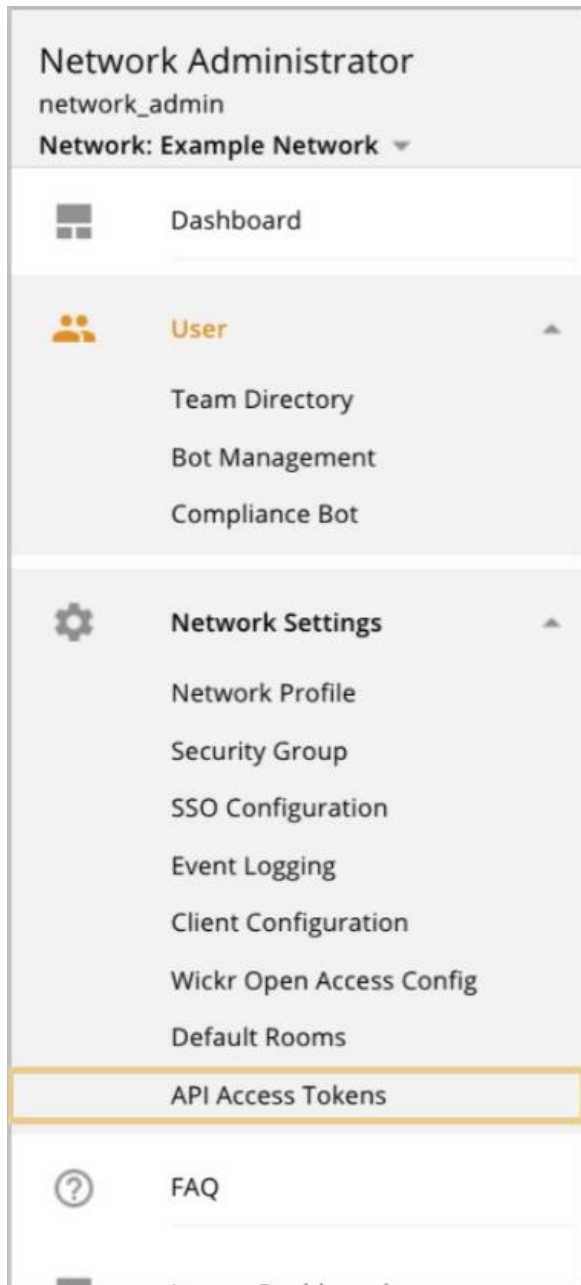
When the Super Administrator has enabled this option, Network

Administrators can create rooms managed by a Bot. This Bot will automatically add users to a room. If the users leave the room, they will be re-added.

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	Security Group: default
<p>All users in this network will automatically be put in this room. Be careful when using this with large networks.</p>	<p>Users assigned to this security group will automatically be put in this room.</p>
<p>Title</p> <input type="text"/>	<p>Title</p> <input type="text"/>
<p>Description</p> <input type="text"/>	<p>Description</p> <input type="text"/>
<p>Message Expiration</p> <p>select message expiration</p>	<p>Message Expiration</p> <p>select message expiration</p>
<p>Messages in this room will be deleted for all users after this time.</p>	<p>Messages in this room will be deleted for all users after this time.</p>
<p>Message Burn On Read</p> <p>off</p>	<p>Message Burn On Read</p> <p>off</p>
<p>Messages in this room will be deleted for all users after this time.</p>	<p>Messages in this room will be deleted for all users after this time.</p>
<p>CREATE A ROOM FOR THIS GROUP</p> <p>INACTIVE</p>	<p>CREATE A ROOM FOR THIS GROUP</p> <p>INACTIVE</p>



API Access

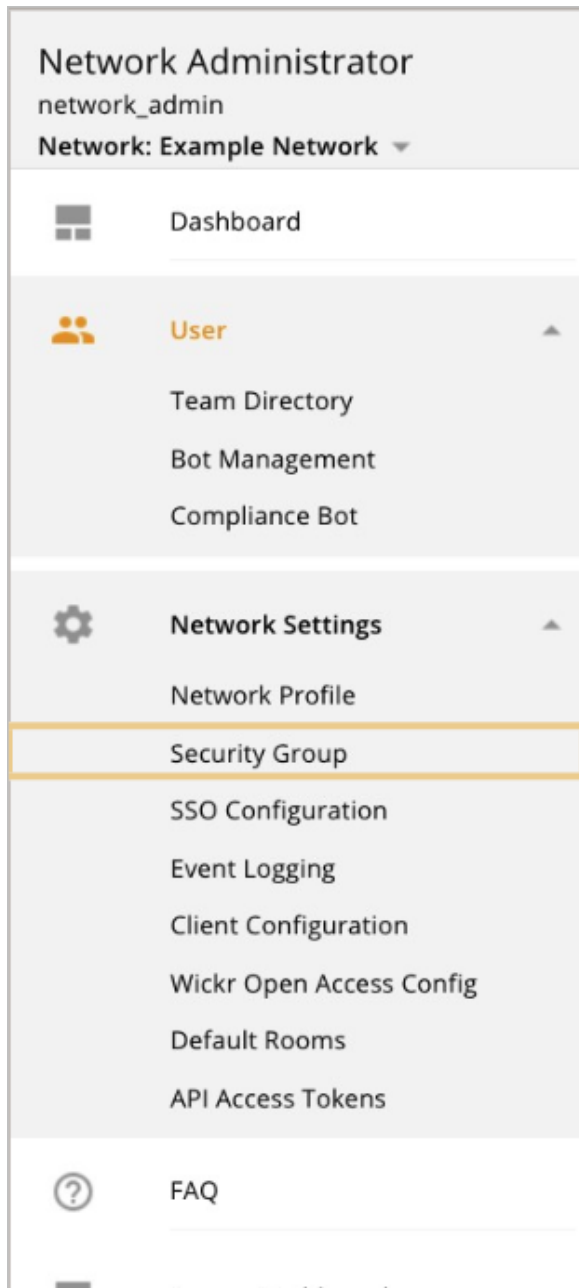
The API Access Token page allows an Administrator to manage API Tokens.

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



Click **Endpoint Documentation** for Complete API documentation. No online access is needed and examples can be generated to quickly test an endpoint using CURL.



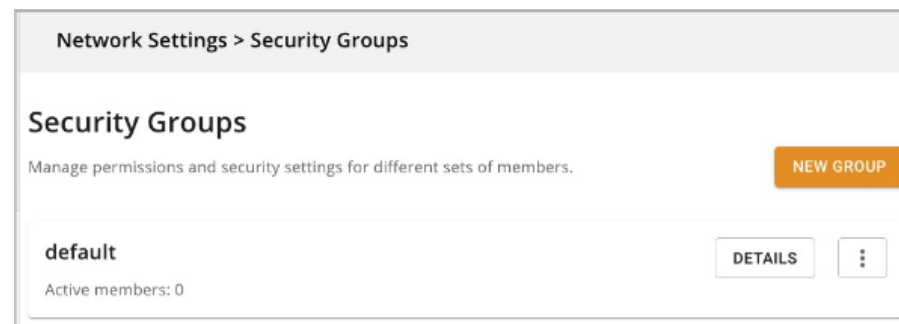


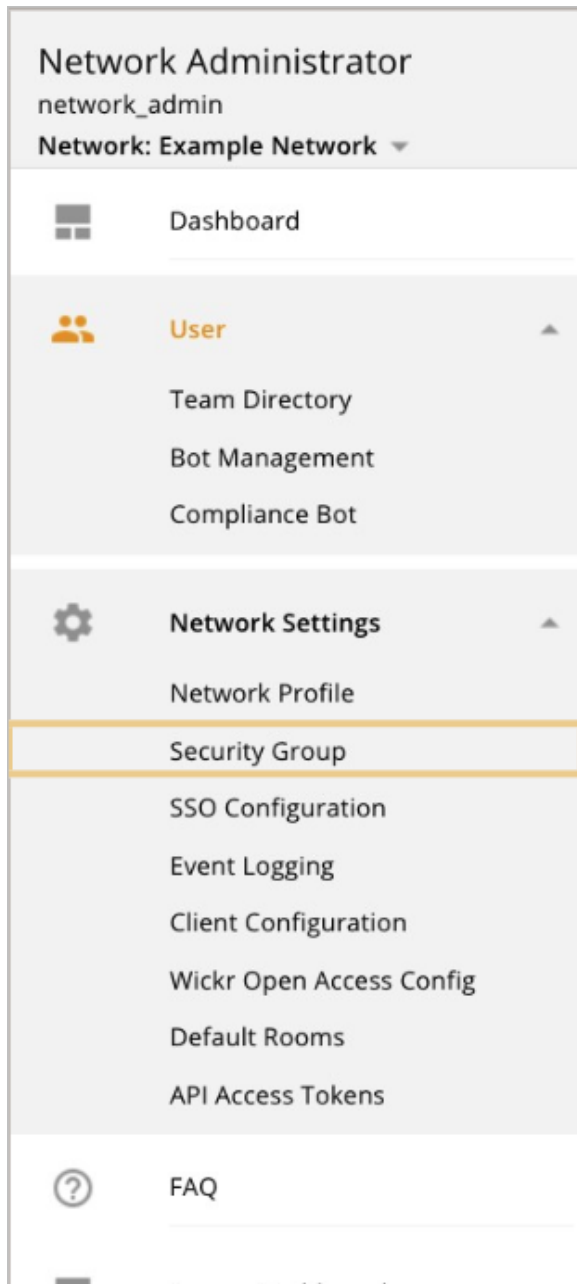
Security Groups

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.

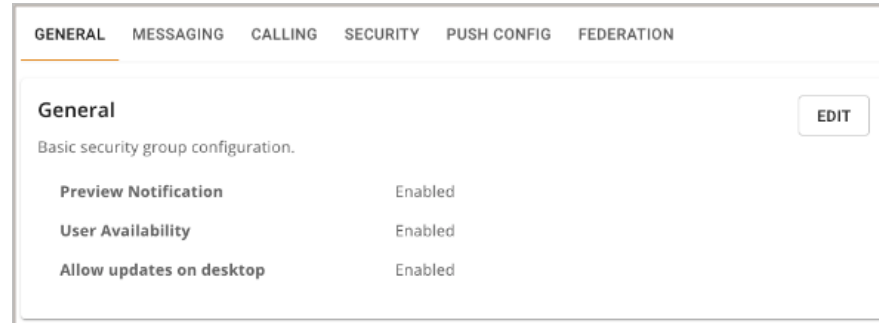


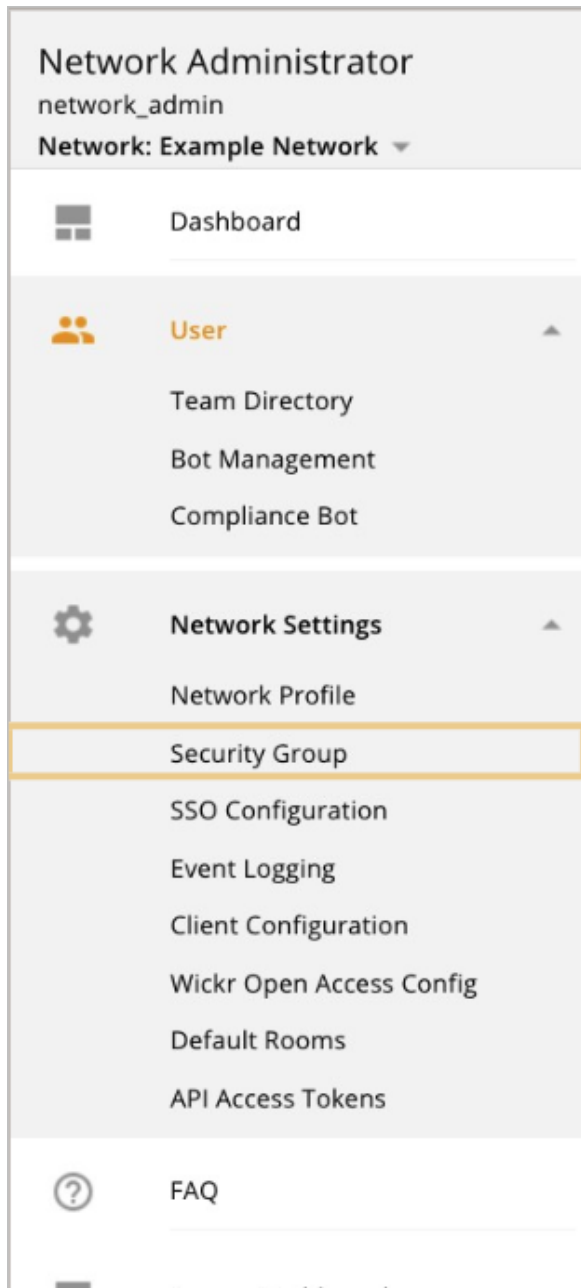


General

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.



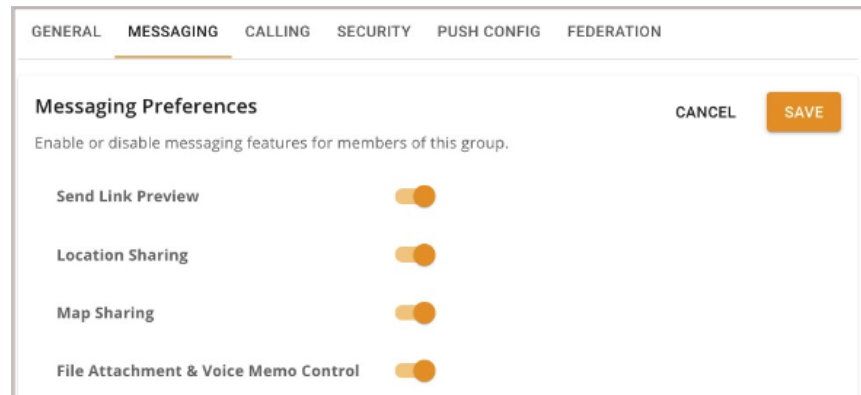


Messaging

The messaging tab has the following available features for users:

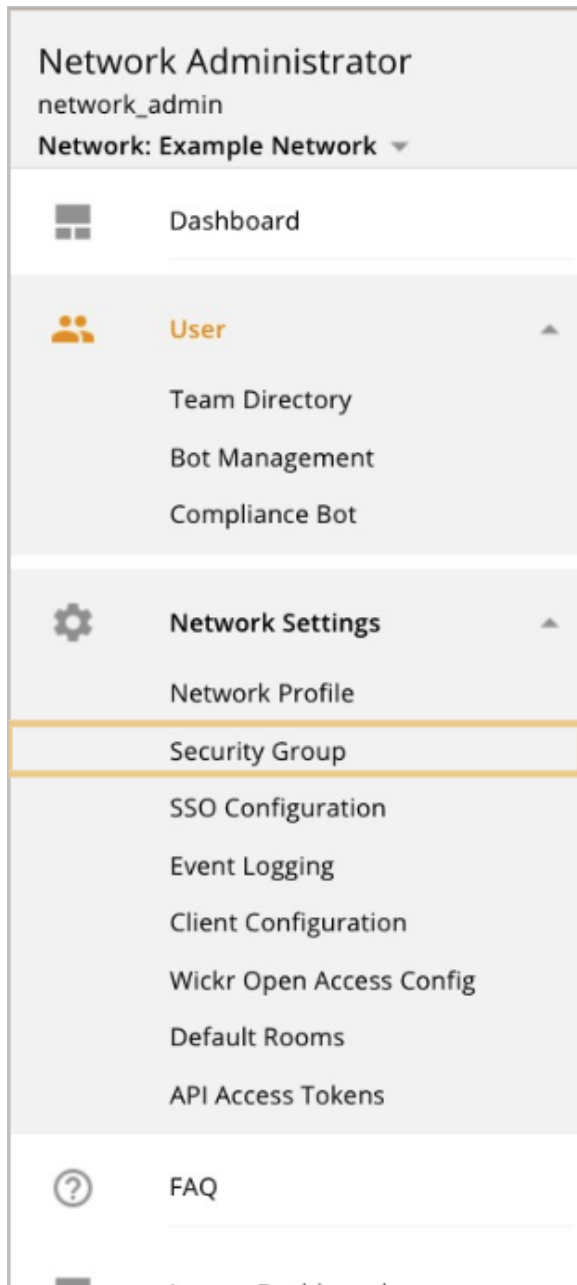
- **Send Link Preview:** This allows a user to send or receive previews for URLs sent within Wickr. The preview is generated from the sending device. Recipients will not connect to the underlying URL until clicked.
- **Location Sharing:** Allows users to share a link to their GPS coordinates in the app.
- **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.

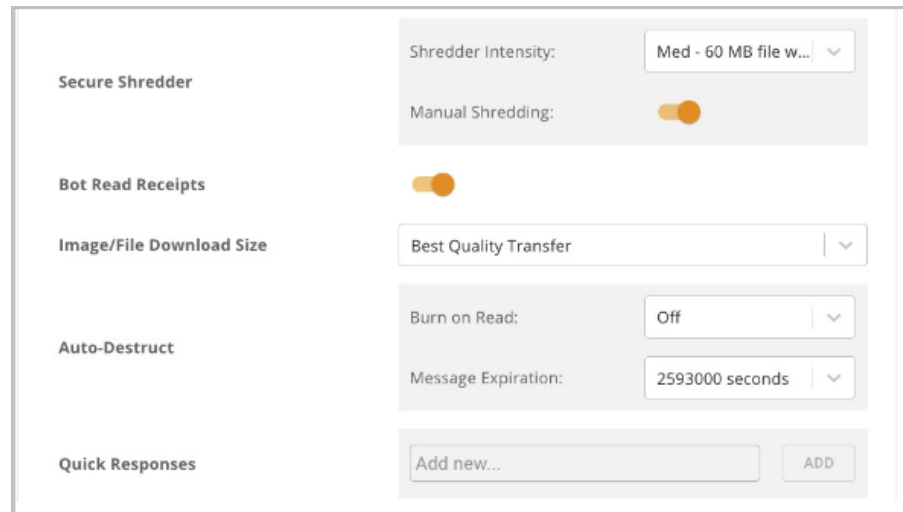


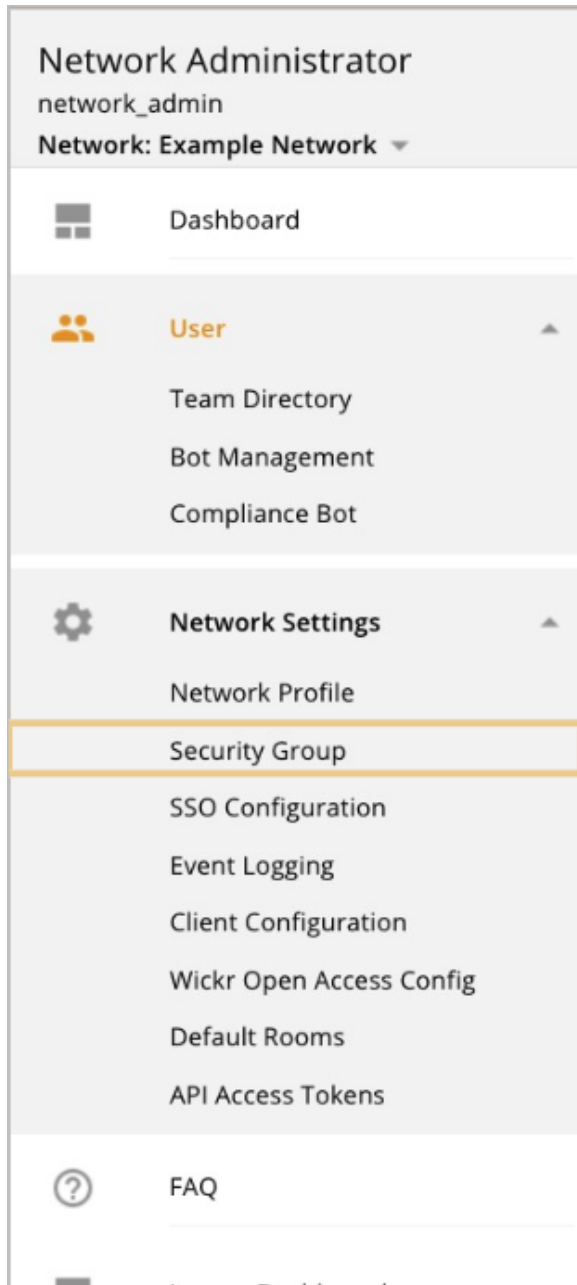
The **Messaging** tab has the following additional features:

- **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.

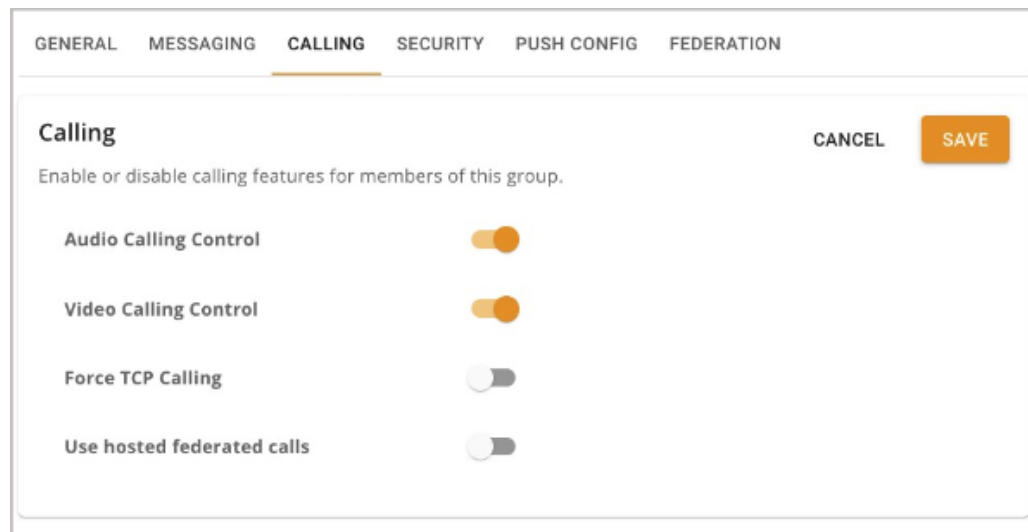


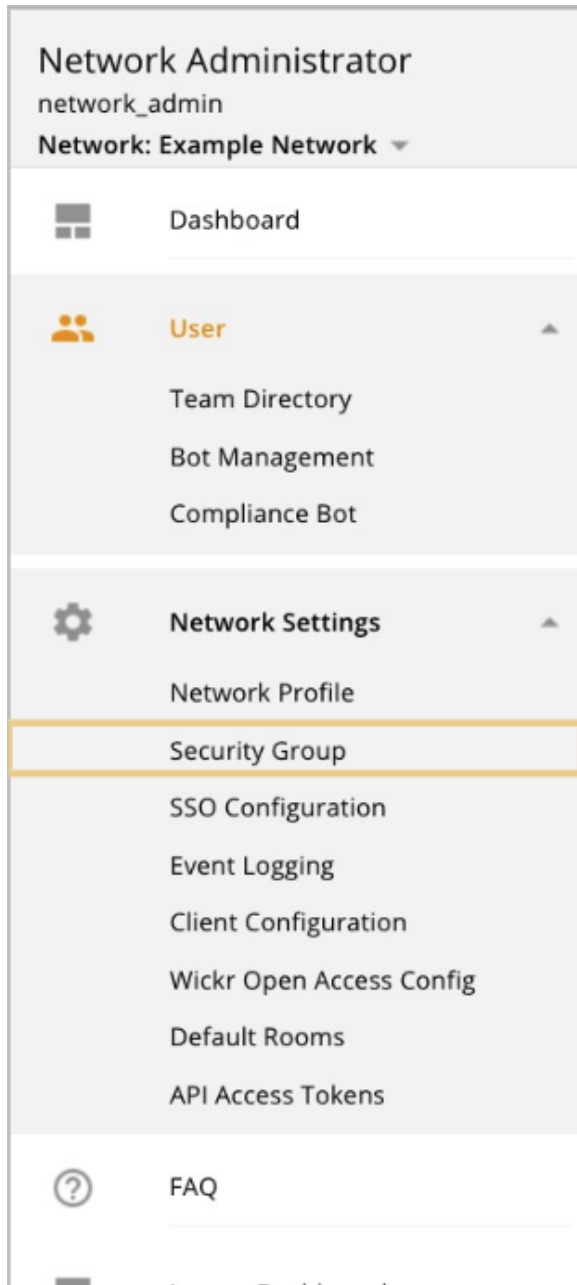


Calling

The **Calling** tab has the following available features for users:

- **Audio Calling Control:** This control 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.



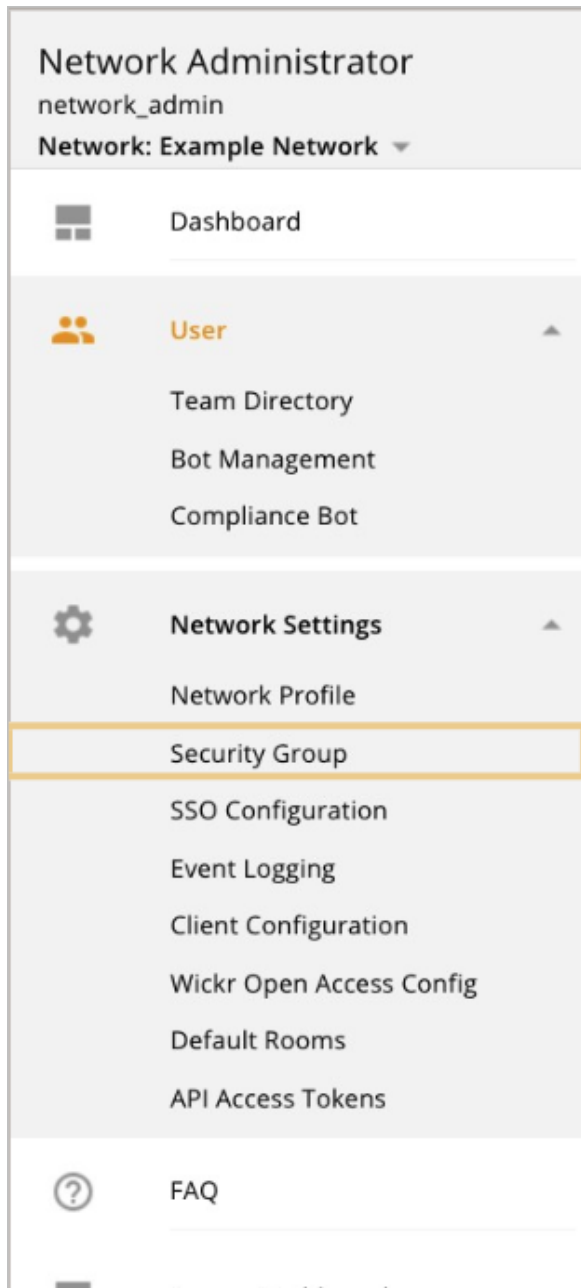


Security

The security tab has the following available options for administration:

- **Always Re-authenticate:** 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:** 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.

Setting	Value
Always Re-authenticate	Disabled
User Password Permission	Enabled
Minimum password length	8
Lowercase letter	0
Uppercase letter	0
Number	0
Special character	0
Device reset	11
User account suspension	10

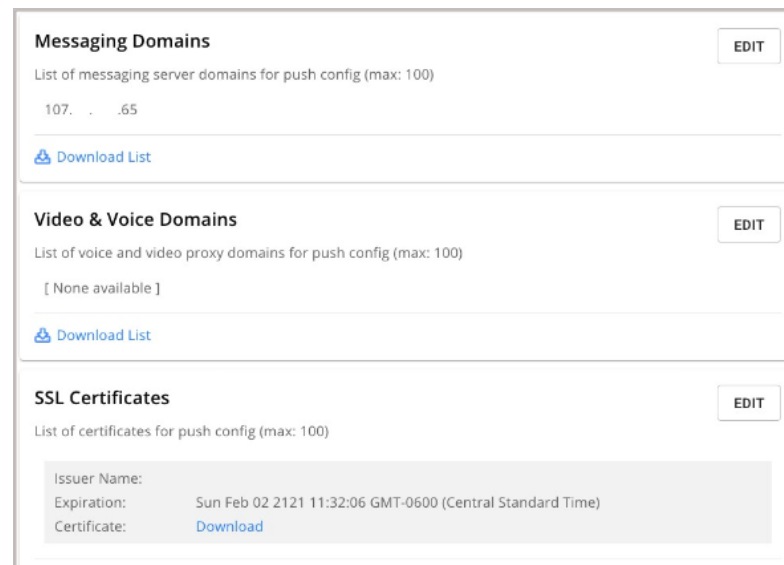


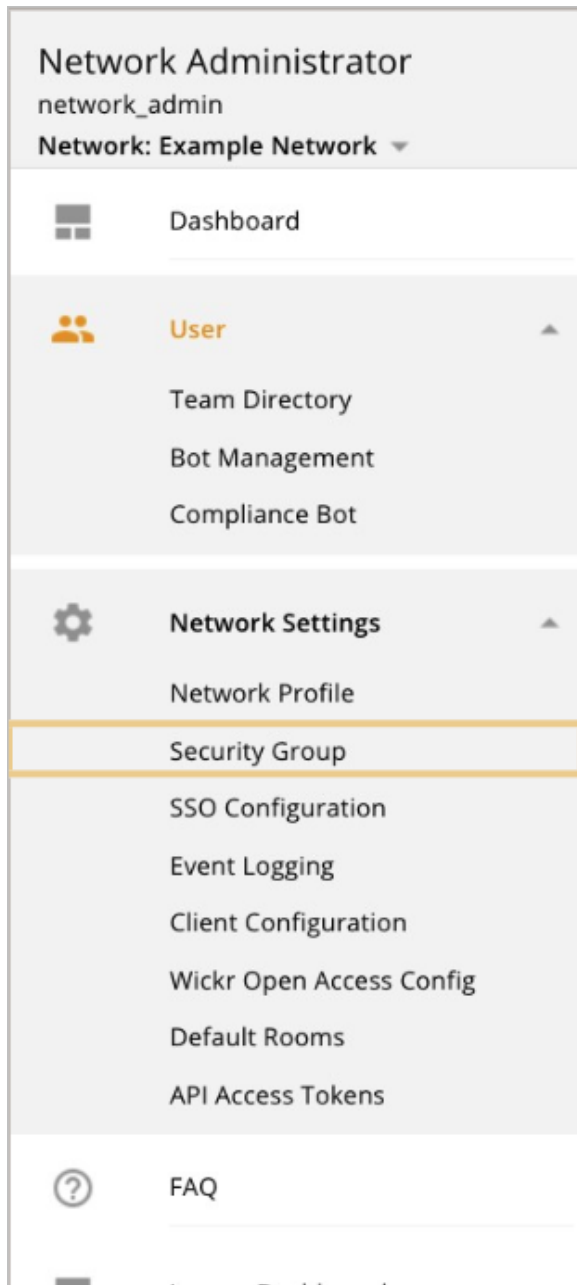
Push Configuration

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.

Note: 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.
- SSL Certificates: The SSL certificate used during installation is here automatically.
- We recommend using intermediate certificates here instead of a leaf





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.

A screenshot of the Federation configuration page. The page has tabs for GENERAL, MESSAGING, CALLING, SECURITY, PUSH CONFIG, and FEDERATION. The FEDERATION tab is active. The page title is 'Federation' with 'CANCEL' and 'SAVE' buttons. Below the title is the text 'Allow your users to communicate across other networks.' The configuration options are: 'Local Federation' with a dropdown menu showing 'Restricted federation'; 'Permitted Networks' with an input field containing 'Add new...' and an 'ADD' button; and 'Global Federation' with a toggle switch that is currently turned on.