Configuring Parallels RAS to work with Rublon MFA Provider

- Parallels Remote Application Server

This article describes how to set up Rublon MFA in Parallels RAS.

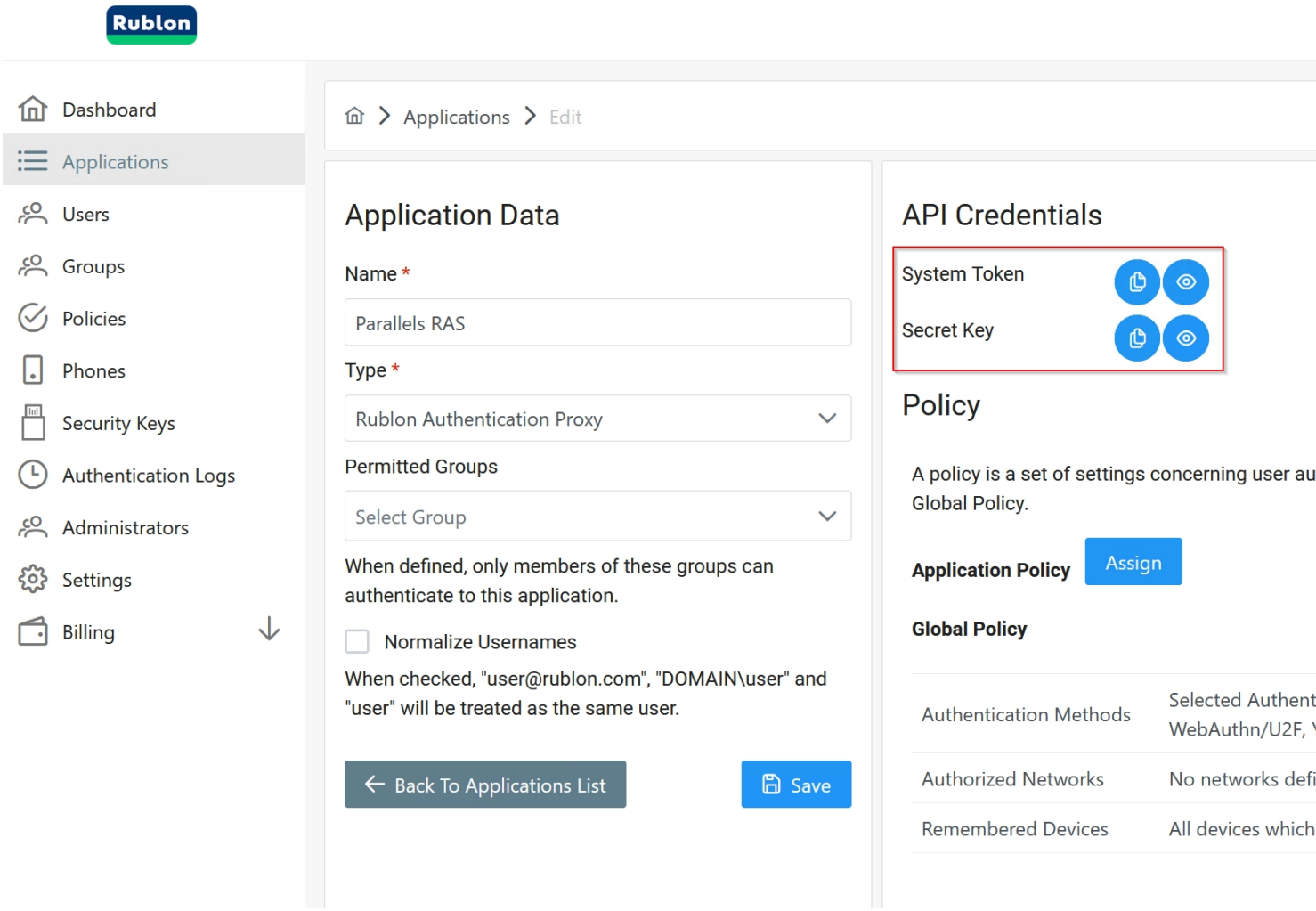
1. Sign up for the Rublon Admin Console.

2. In the Rublon Admin Console, go to the **Applications** tab and click **Add Application**.

3. Enter a name for your application (e.g., **Parallels RAS)** and then set the type to **Rublon Authentication Proxy**.

4. Click **Save** to add the new application in the Rublon Admin Console.

5. Copy and save the values of the **System Token** and **Secret Key**.



6. Install the Rublon Authentication Proxy

7. Open **Windows Explorer**, navigate to `C:\Program Files\Rublon Security Auth Proxy\config` and open `config.json`.

8. For typical RAS integration, we should configure the following sections:

PROXY:

`RUBLON_API` – Rublon API host (core.rublon.net);

`RADIUS_SECRET` - The secret key that you will specify in step **12**;

SERVERS:

`IP` - IP address of RADIUS server with installed Rublon Authentication Proxy

`PORT` - Port on which to listen for incoming RADIUS Access Requests. By default, the proxy will listen on port **1812**;

`MODE` - Have to be used **"nocred"**;

`AUTH_SOURCE` - Indicates which authentication source should be used for primary authentication, usually **“LDAP”**;

`RUBLON_TOKEN` - Token of an application saved in step **5**;

`RUBLON_SECRET` - Secret of an application added in step **5**;

`AUTH_METHOD` - Authentication method used for 2FA. Valid options are **“push”** and **“email”**;

LDAP:

`HOST` - Hostname or IP address of Active Directory used for primary authentication;

`SEARCH_DN` - The LDAP distinguished name (DN) of an Active Directory container or organizational unit (OU) containing all of the users you wish to permit to log in;

`ACCESS_USER_DN` - The full Bind distinguished name (DN) of a user with Read rights in Active Directory. This account will be used for user search;

`ACCESS_USER_PASSWORD` - The password corresponding to service_account_username;

RADIUS:

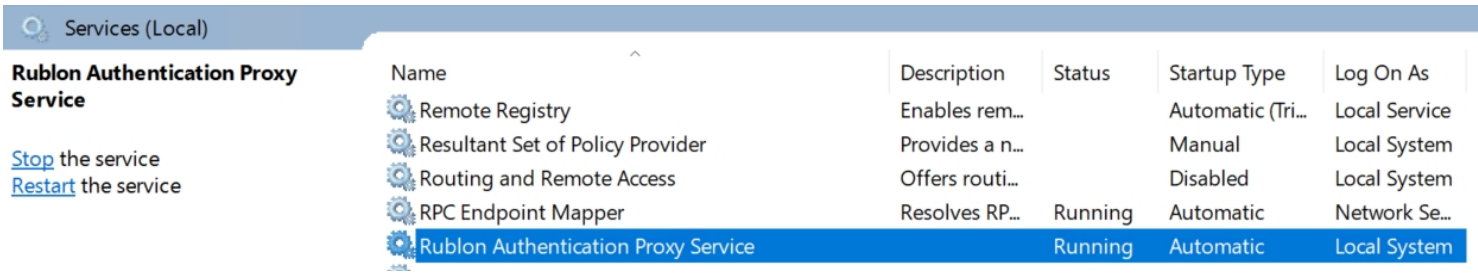
`SERVER_IP` - IP address of RAS Connection Broker;

`PORT` - Port on which to listen for incoming RADIUS Access Requests. By default, the proxy will listen on port **1812**;

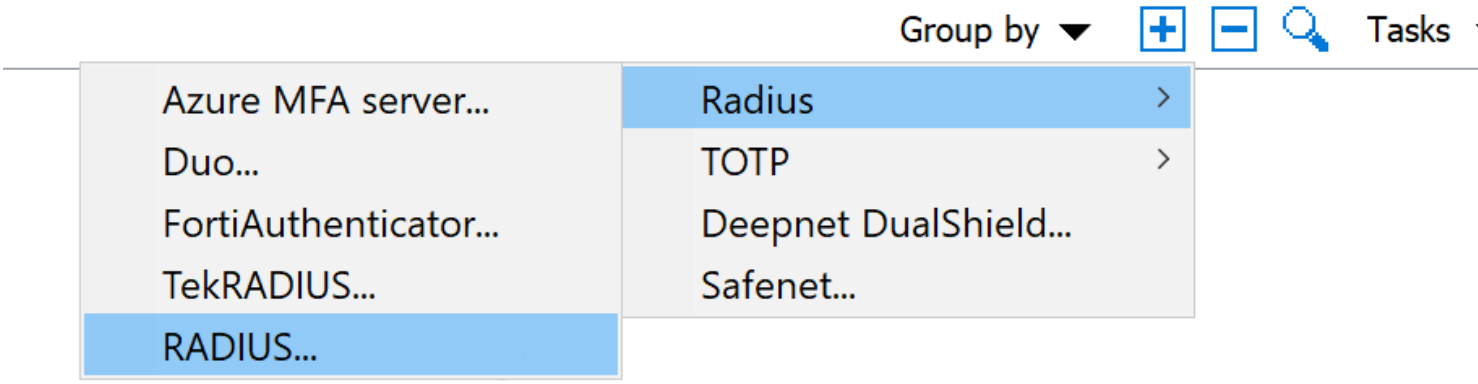
Example of config.json:

```
{
  "PROXY": {
    "RADIUS_SECRET": "[redacted]",
    "RUBLON_API": "https://core.rublon.net",
    "SERVERS": [
      {
        "IP": "10.10.10.5",
        "PORT": 1812,
        "MODE": "nocred",
        "AUTH_SOURCE": "LDAP",
        "RUBLON_TOKEN": "[redacted]",
        "RUBLON_SECRET": "[redacted]",
        "AUTH_METHOD": "push,email"
      }
    ]
  },
  "LDAP": {
   "HOST": "10.10.10.1",
   "SEARCH_DN": "dc=ras,dc=local",
   "ACCESS_USER_DN": "cn=Administrator,cn=Users,dc=ras,dc=local",
   "ACCESS_USER_PASSWORD": "[redacted]"
  },
  "RADIUS": {
    "SERVER_IP": "10.10.10.2",
    "PORT": 1812
  }
}
```

9. Start **Rublon Authentication Proxy Service**:

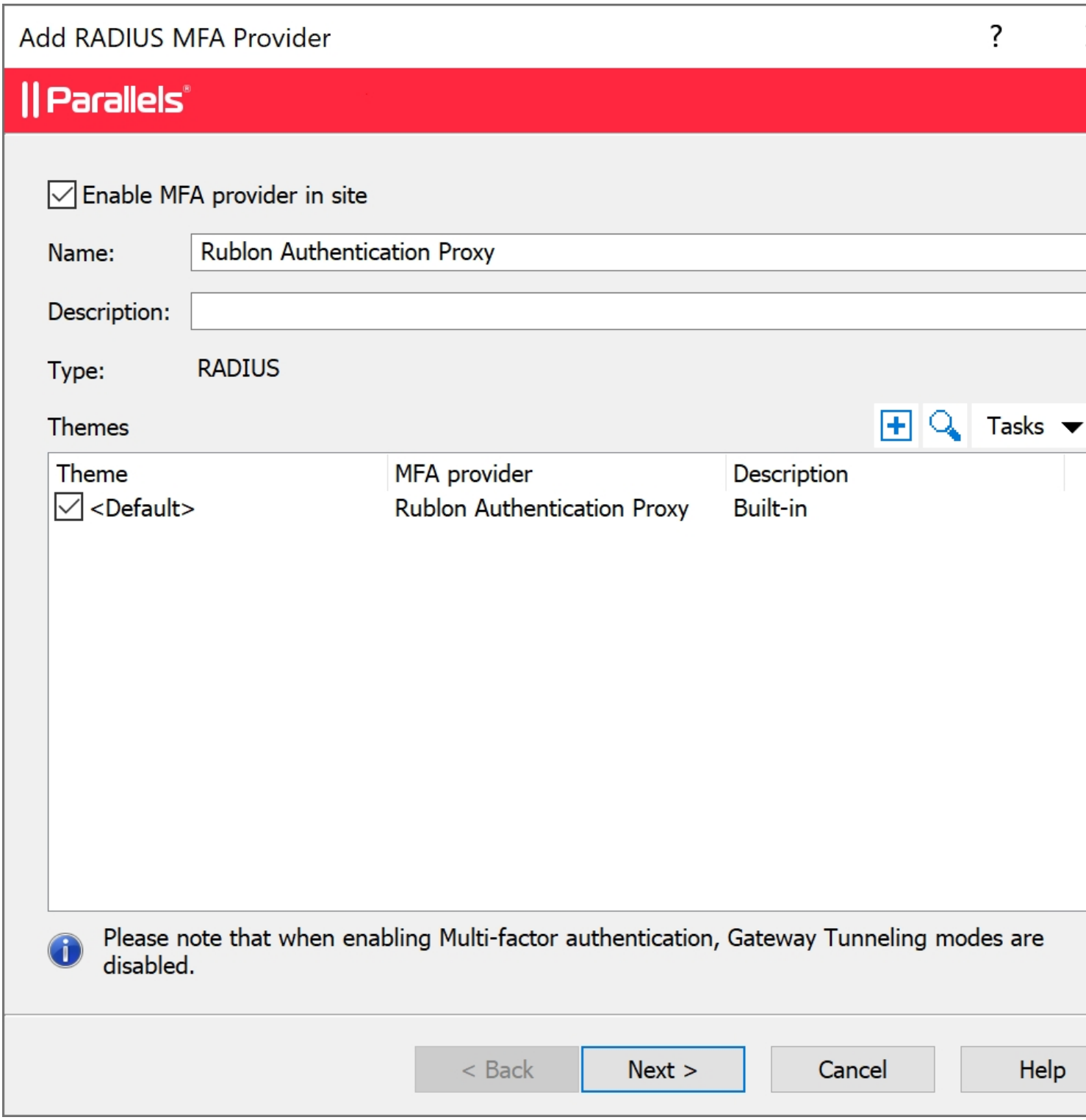


10. Configure RAS to communicate with Duo: **RAS Console** **Connections** **Multi-Factor Authentication** Tab. Click the **+** (plus) icon in the upper-right corner and then select **RADIUS** **RADIUS…**:



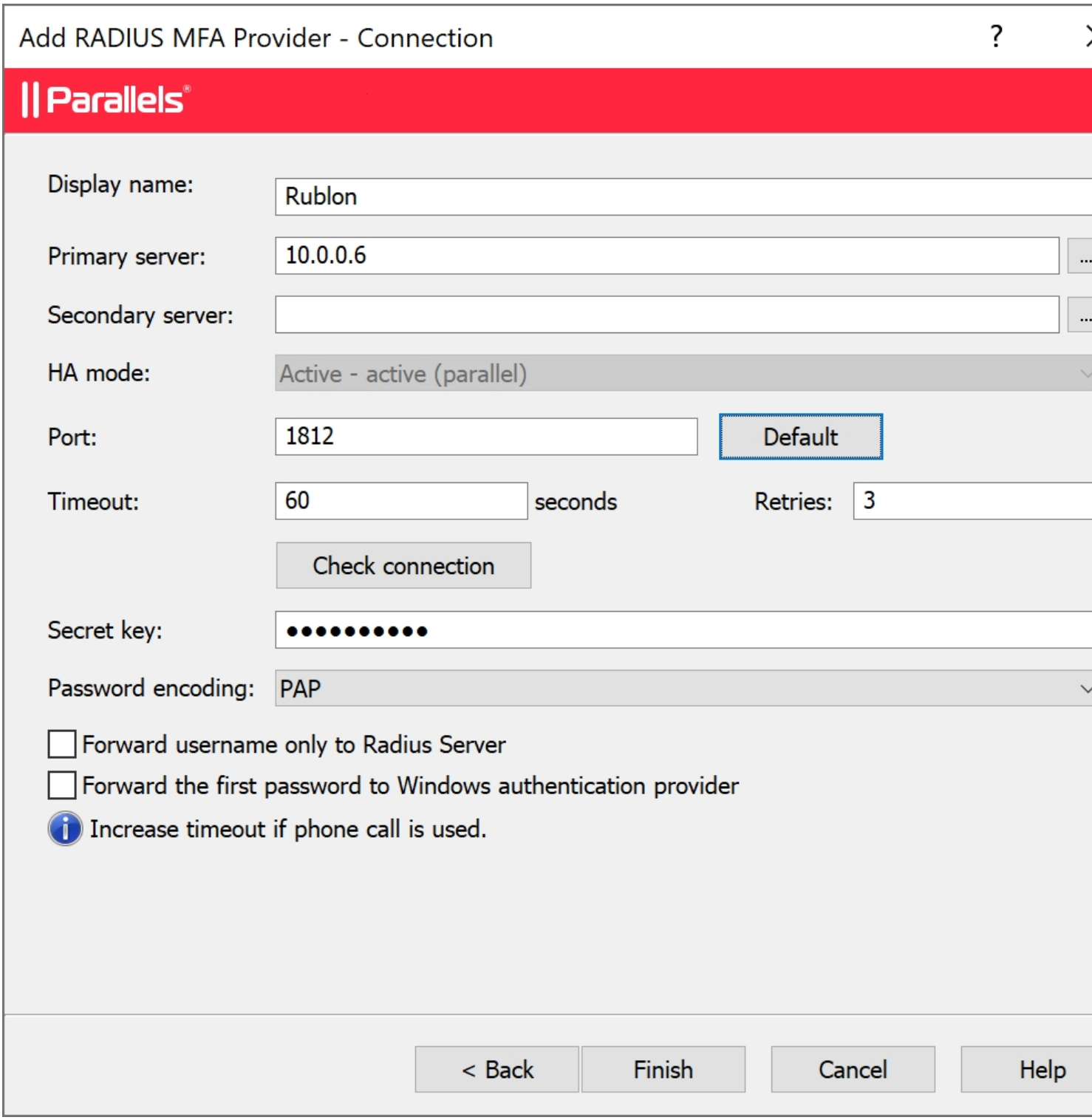
11. In the new window, enter the following information:

- **Name**: Name for your RADIUS server (e.g., **Rublon Authentication Proxy**)
- **Description**: Optional description for your RADIUS server
- **Themes**: Select a theme for Rublon MFA.



12. Configure connection settings:

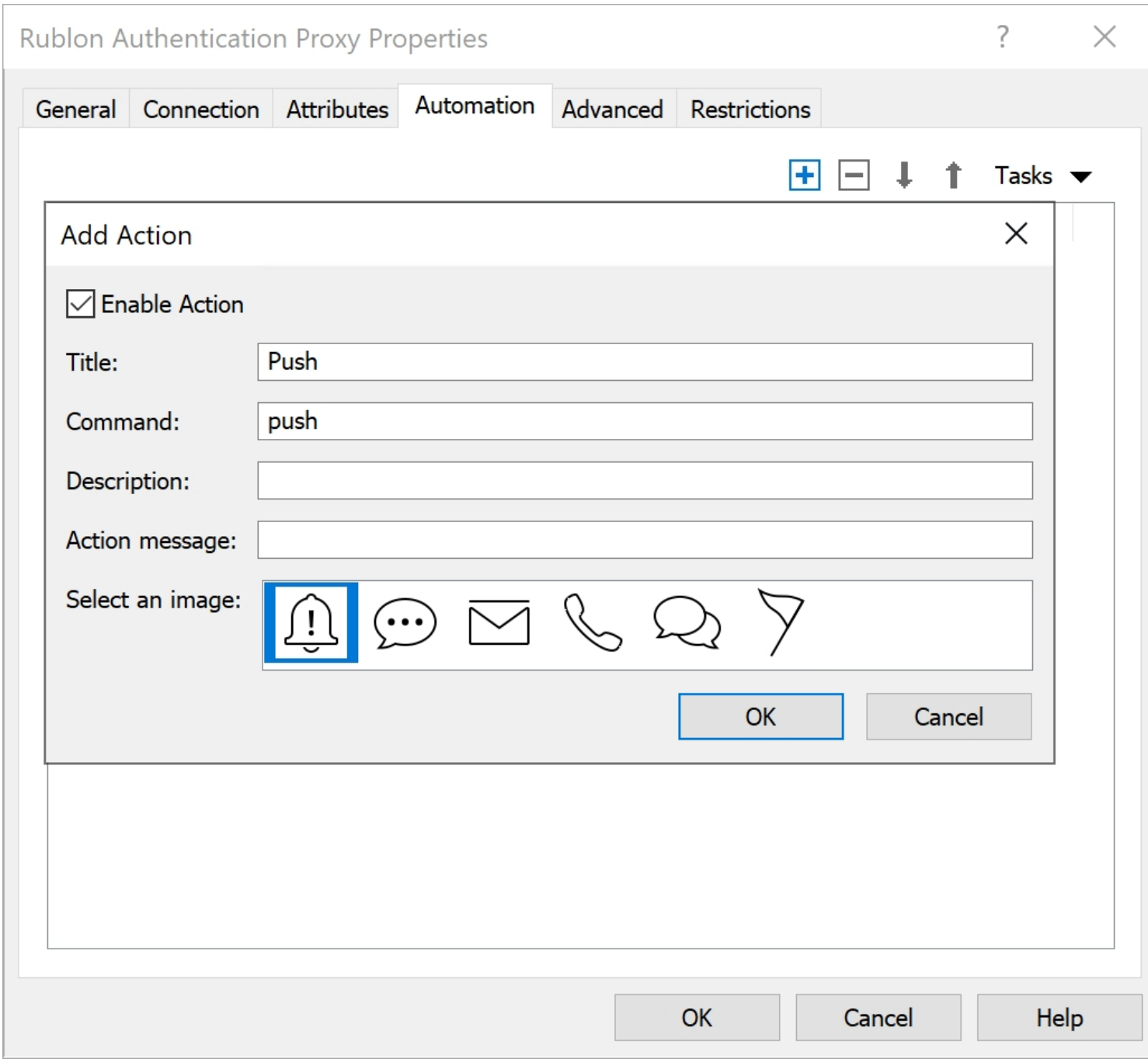
- **Primary Server**: Server where Rublon Authentication Proxy is installed.
- **Port**: Port from step **8**, usually **1812**.
- **Secret key**: `RADIUS_SECRET` from step **8**.



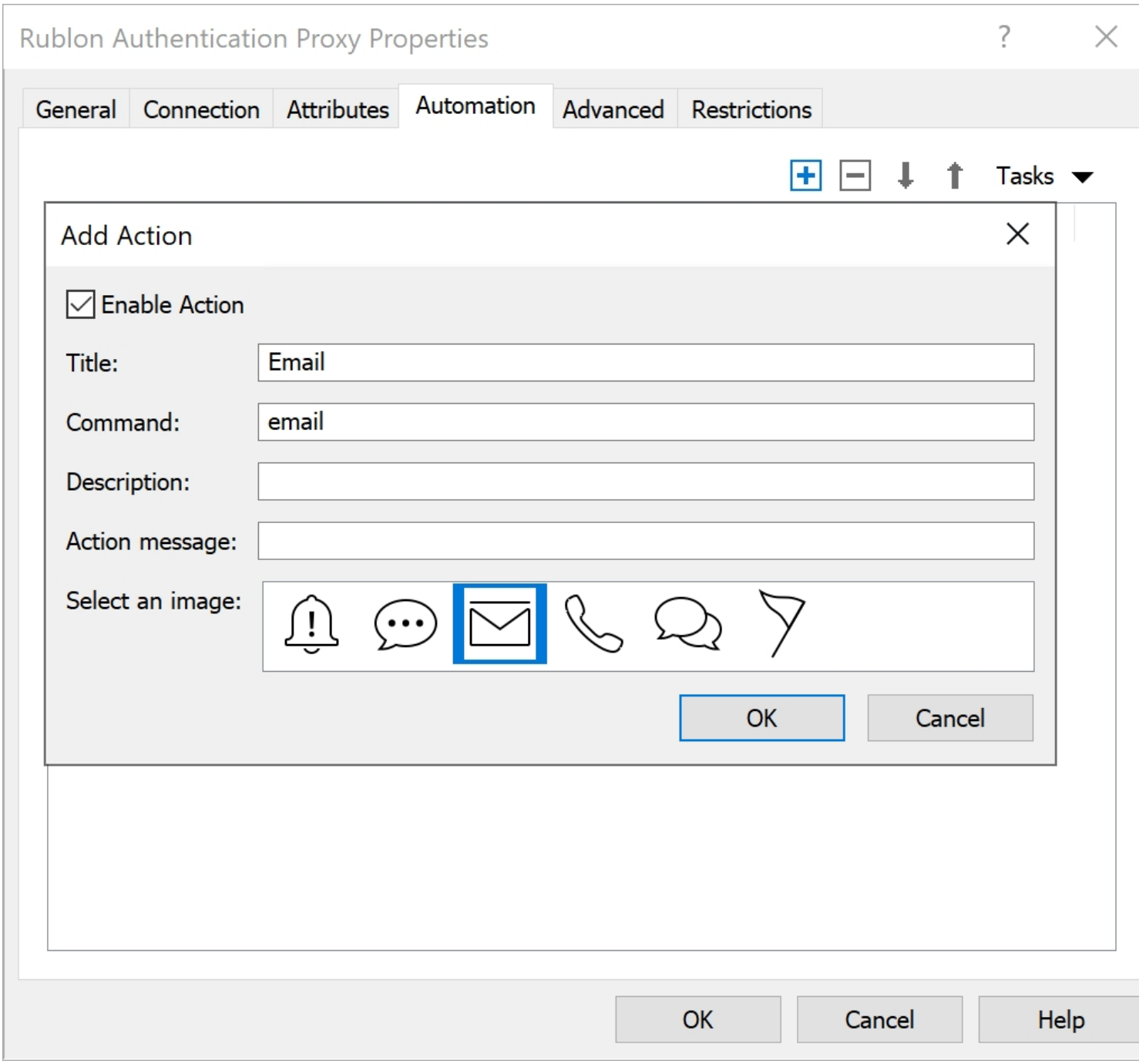
13. Click **Finish** to save your RADIUS MFA provider configuration.

14. To enable Mobile Push and Email Link authentication methods on the **Multi-Factor authentication** tab, double-click the RADIUS server. In the opened window, go to the **Automations** tab.

15. Click the **+** (plus) icon in the upper-right corner and fill in the form for the Push method:

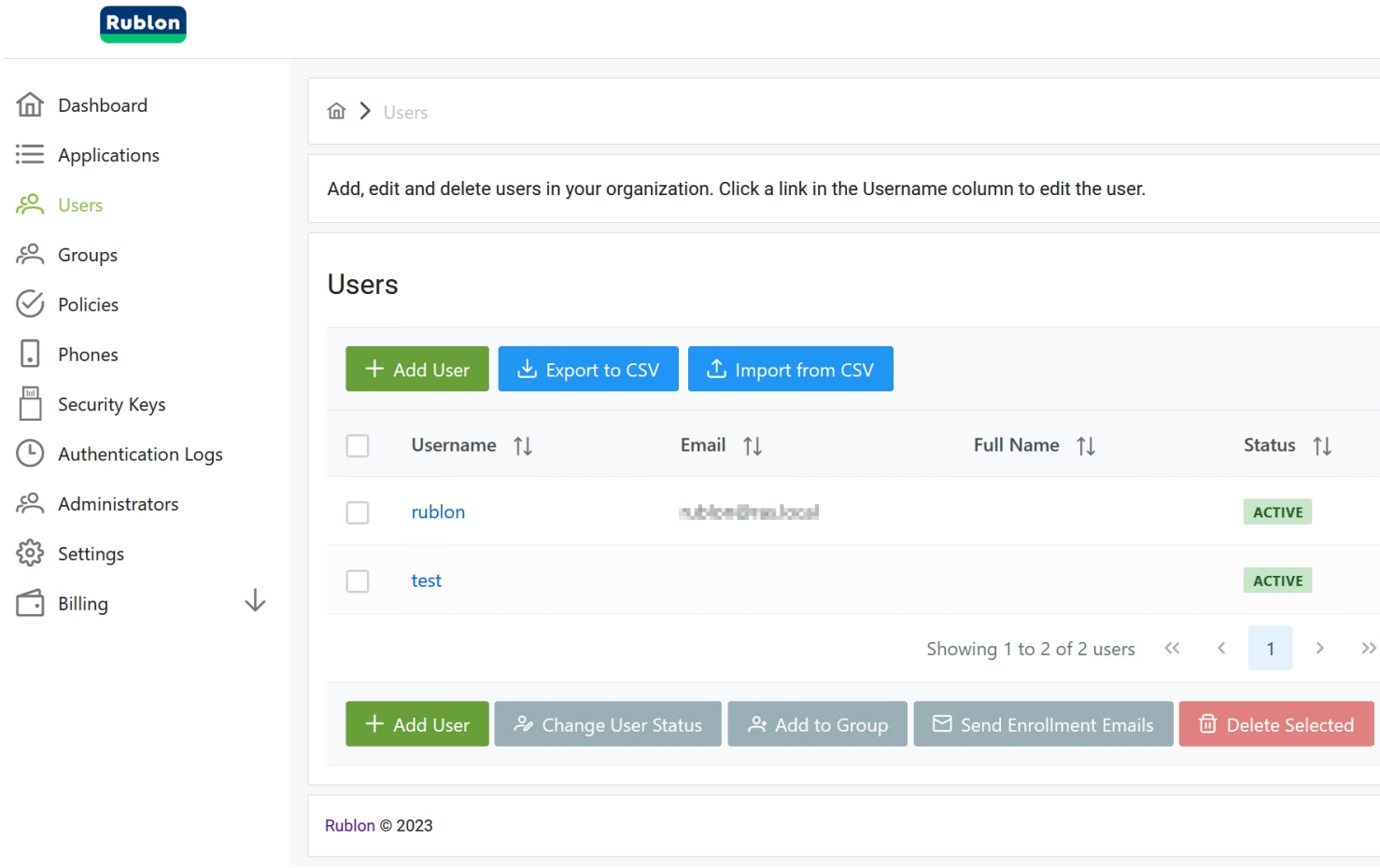


16. Click the **+** (plus) icon in the upper-right corner and fill in the form for the Email method:



17. Click **OK** **Apply**

18. Add users to Rublon Admin Console:



19. Next time users log on to RAS Client, a window will appear with the authentication methods to choose: