

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**.

The screenshot shows the Rublon Admin Console interface. On the left is a sidebar with navigation links: Dashboard, Applications (selected), Users, Groups, Policies, Phones, Security Keys, Authentication Logs, Administrators, Settings, and Billing. The main content area is titled 'Applications > Edit'. It is divided into three sections: 'Application Data', 'API Credentials', and 'Policy'. The 'Application Data' section contains fields for 'Name' (Parallels RAS), 'Type' (Rublon Authentication Proxy), 'Permitted Groups' (Select Group), and a checkbox for 'Normalize Usernames'. The 'API Credentials' section has fields for 'System Token' and 'Secret Key', each with copy and eye icons. The 'Policy' section includes a description, an 'Assign' button, and a table for 'Global Policy' with rows for Authentication Methods, Authorized Networks, and Remembered Devices.

Global Policy	
Authentication Methods	Selected Authent WebAuthn/U2F, Y
Authorized Networks	No networks defi
Remembered Devices	All devices which

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": "1q2w3e4r",
    "RUBLON_API": "https://core.rublon.net",
    "SERVERS": [
      {
        "IP": "10.10.10.5",
        "PORT": 1812,
        "MODE": "nocred",
        "AUTH_SOURCE": "LDAP",
        "RUBLON_TOKEN": "60585884a745400944a2a831257c44b83",
        "RUBLON_SECRET": "ed231f4420480c8f652a793179182a274",
        "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": "1q2w3e4r"
  },
  "RADIUS": {
    "SERVER_IP": "10.10.10.2",
    "PORT": 1812
  }
}
```

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

Services (Local)					
Rublon Authentication Proxy Service Stop the service Restart the service					
Name	Description	Status	Startup Type	Log On As	
Remote Registry	Enables rem...		Automatic (Tri...	Local Service	
Resultant Set of Policy Provider	Provides a n...		Manual	Local System	
Routing and Remote Access	Offers routi...		Disabled	Local System	
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network Se...	
Rublon Authentication Proxy Service		Running	Automatic	Local System	

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...**:

Azure MFA server...

Duo...

FortiAuthenticator...

TekRADIUS...

RADIUS...

Radius >

TOTP >

Deepnet DualShield...

Safenet...

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.



☒ Enable MFA provider in site

Name: Rublon Authentication Proxy

Description:

Type: RADIUS

Themes



Tasks ▼

Theme	MFA provider	Description
☒ <Default>	Rublon Authentication Proxy	Built-in



Please note that when enabling Multi-factor authentication, Gateway Tunneling modes are disabled.

< Back

Next >

Cancel

Help

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.

Add RADIUS MFA Provider - Connection

?

...

Parallels®

Display name:

Rublon

Primary server:

10.0.0.6

Secondary server:

HA mode:

Active - active (parallel)

Port:

1812

Default

Timeout:

60

seconds

Retries:

3

Check connection

Secret key:

●●●●●●●●

Password encoding:

PAP

☐ Forward username only to Radius Server

☐ Forward the first password to Windows authentication provider

 Increase timeout if phone call is used.

< Back

Finish

Cancel

Help

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:

Rublon Authentication Proxy Properties

General Connection Attributes Automation Advanced Restrictions

+ - ↓ ↑ Tasks ▼

Add Action

☒ Enable Action

Title: Push

Command: push

Description:

Action message:

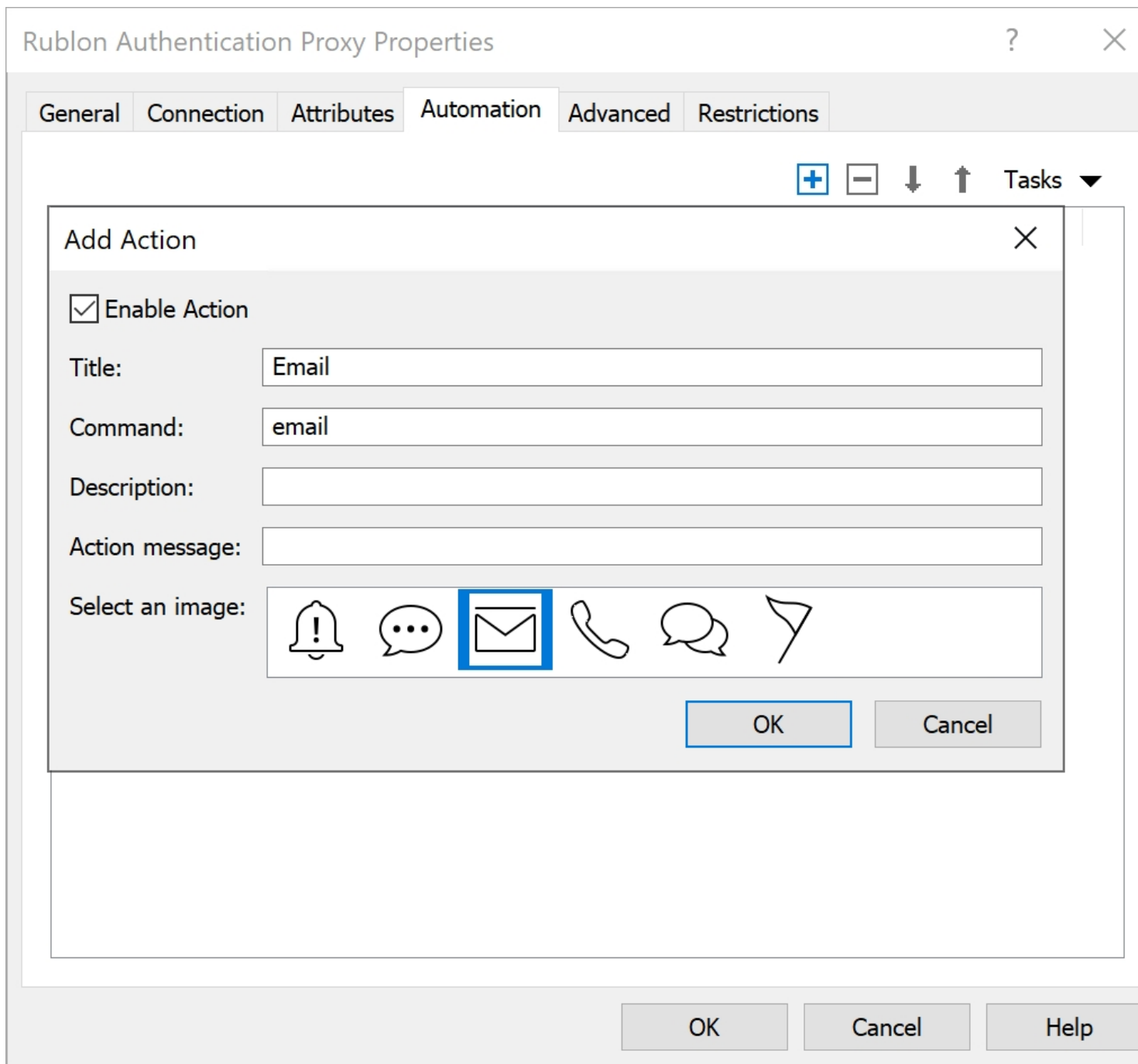
Select an image:

OK Cancel

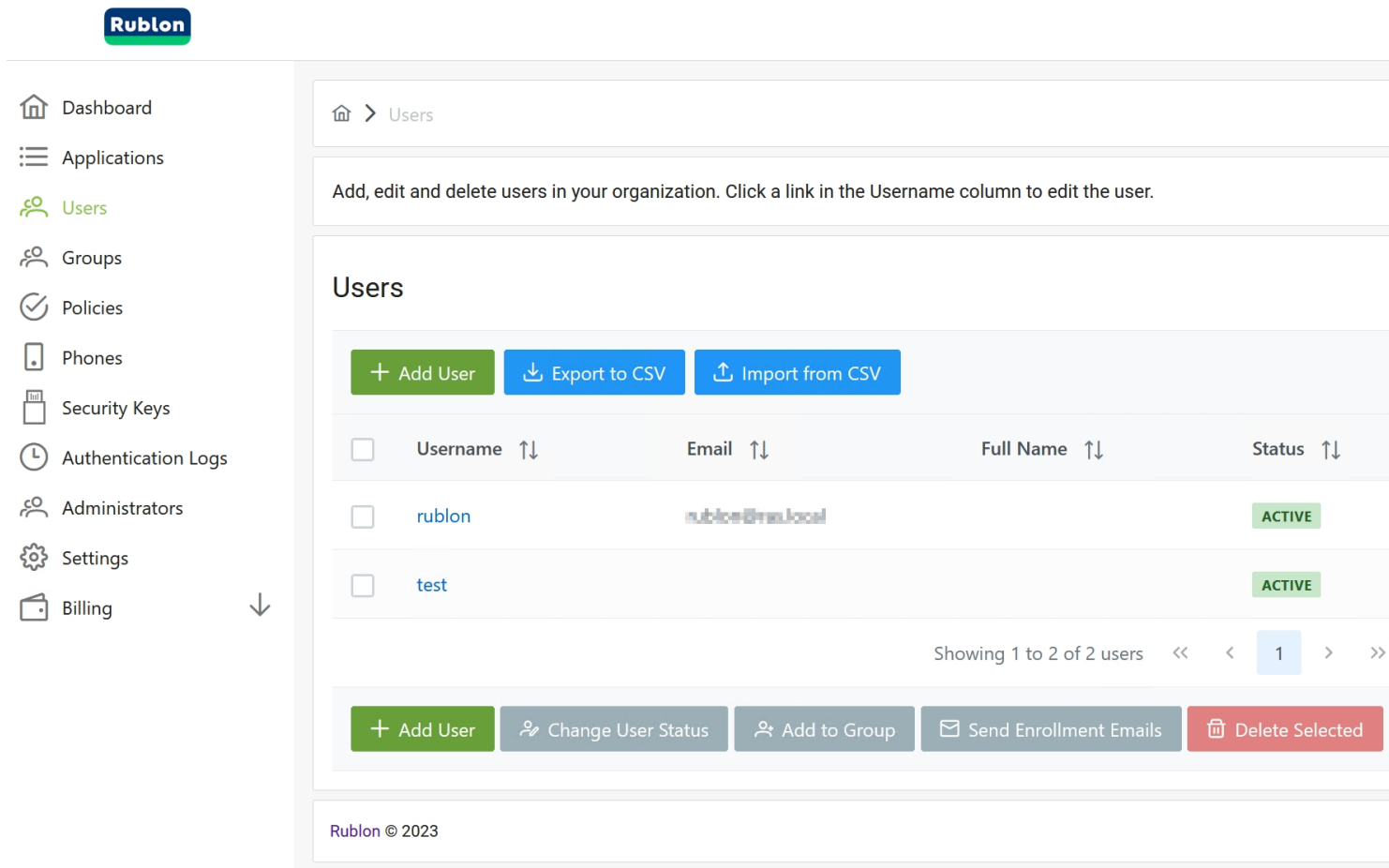
OK Cancel Help

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

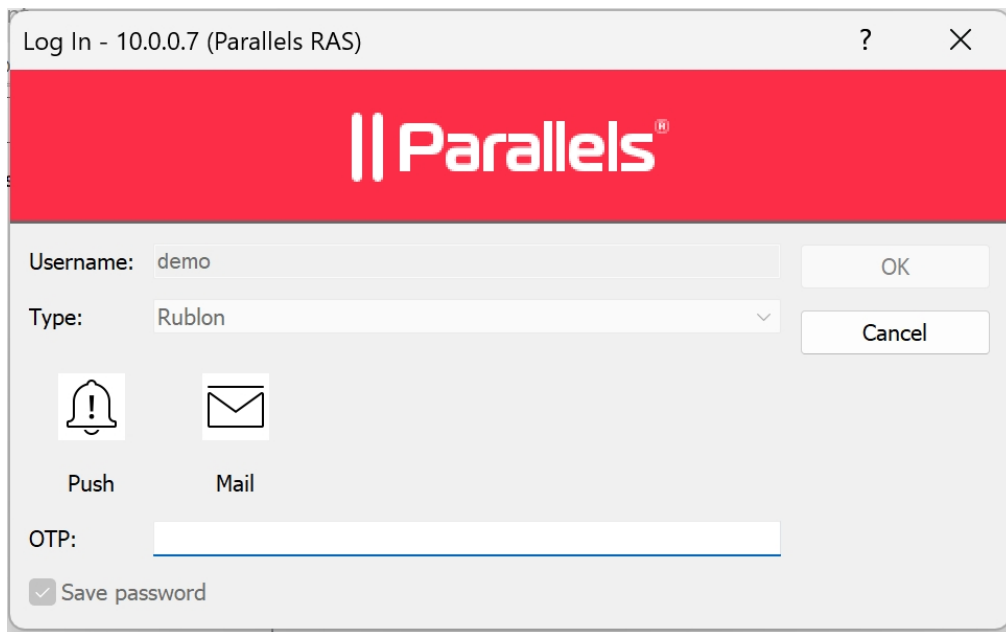


17. Click **OK** **Apply**

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:



© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.