Multiple Multi-factor Authentication (MFA) providers

- Parallels Remote Application Server 19.0
- Parallels Remote Application Server 19.1

Starting from Parallels Remote Application Server 19, multiple Multifactor Authentication providers can be configured in a Site and enabled or disabled for users using Parallels RAS Themes.

Note: v19.2 includes Microsoft Authenticator as an MFA option under TOTP:

- RADIUS
  - Azure MFA (RADIUS)
  - Duo (RADIUS)
  - FortiAuthenticator (RADIUS)
  - TekRADIUS
  - Other RADIUS providers
- TOTP
  - Google Authenticator
  - Microsoft Authenticator
  - Other TOTP providers
- Deepnet DualShield
- Safenet

Configuration

To create a new MFA, provide:

1. In the RAS Console, navigate to **Connection** and select the **Multi-Factor Authentication** tab.
2. Click **Tasks > Add** (or click the **[+]** icon).
3. Select your MFA provider. A wizard will open.
4. In the Wizard window, specify the following parameters:
   - **Name**: Name of the provider.
   - **Description**: Description of the provider.
   - In the **Themes** table, select the Themes that will use this MFA provider.
5. Click **Next**.
6. Do one of the following
   - If you use RADIUS, configure it as described in https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/40120.htm.
   - If you are using TOTP, specify the following: https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/48418.htm
   - **Display name**: Name of the provider.
   - The **User enrollment** section allows you to limit user enrollment if needed. You can allow all users to enroll without limitations (the **Allow** option), allow enrollment until the specified date and time (**Allow until**), or completely disable enrollment (the **Do not allow** option).
   - The **Authentication** section allows you to configure TOTP tolerance. When using Time based One-Time Password (TOTP), it is required to have the time synchronized between the RAS Publishing Agent and client devices. The synchronization must be performed against a global NTP server (e.g. time.goole.com). Using the TOTP tolerance drop-down box, you can select a time difference that should be tolerated while performing authentication. Expand the drop-down box and select one of the predefined values (number of seconds). Note that changing

time tolerance should be used with caution as it has security implications since the time validity of a security token can be increased, thus a wider time window for potential misuse.
Note: When using Time-based One-time Passwords (TOTP) providers, it is required to have both Publishing Agents' and client devices' time synchronized with a global NTP server (e.g. time.google.com). Adding TOTP tolerance increases the one-time password validity, which might have security implications.

- If you are using Deepnet, configure it as described in https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/40134.htm.
- If you are using Safenet, configure it as described in https://download.parallels.com/ras/v19/docs/en_US/Parallels-RAS-19-Administrators-Guide/40123.htm.

To change the themes that use an MFA provider:

1. In the RAS Console, navigate to **Connection** and select the **Multi-Factor Authentication** tab.
2. Right-click on your provider. The **Properties** dialogue will open.
3. In the **Themes** table, select the Themes that will use this MFA provider.
4. Click **OK**.
