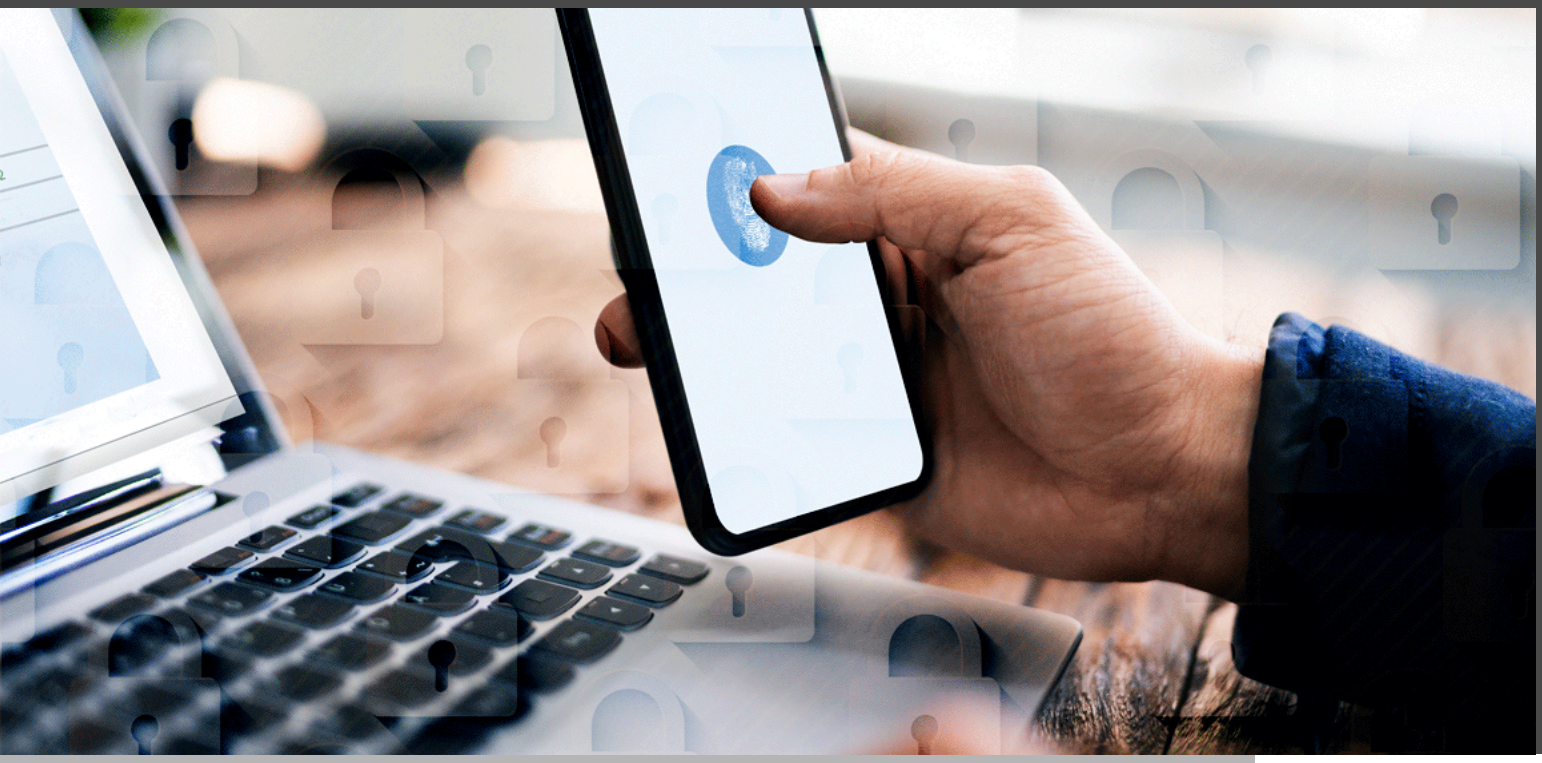
Devolutions

[NEW] Use Case: How Organizations Can Increase Security by Enforcing Specific MFA Tools for Remote Desktop Manager Users



TWO FACTOR AUTHENTICATION (2FA) SUPPORTS UNAMBIGUOUS IDENTIFICATION OF USERS

Two Factor Authentication (2FA) supports unambiguous identification of users through the combination of their assigned credentials (username/password combination) and another component. This could be:

- **Additional login credentials only known to a user**, such as the answer to a security question or a PIN.
- **A code that is delivered on a device that a user physically has in their possession**, such as their smartphone.
- **Biometric login credentials that are unique to the user**, such as retina scans and fingerprints.

However, while 2FA adds another layer of account security, **organizations may not approve of the specific 2FA tool that has been selected by a user or multiple users**. Trying to enforce compliance can be time-consuming and tedious, a drawback that can create significant security vulnerabilities.

Fortunately, **there is a simple and proven solution: integrate Remote Desktop Manager with Devolutions Server**, which supports multiple popular and highly rated 2FA tools, such as Google Authenticator, Yubikey, SMS, and several others. Furthermore, organizations can enforce a default 2FA tool for all users, or enforce a 2FA tool for a specific user or multiple users.

In our new Case Study, **you will discover how integrating Remote Desktop Manager with Devolutions Server:**

- **Enhances security:** Ensure that all users are authenticated through 2FA.
- **Enforces compliance:** Ensure that only selected 2FA tool(s) are valid for logging into Remote Desktop Manager.
- **Supports users:** Allow users (as authorized) to choose from a pool of MFA tools they are familiar with and already use for their personal accounts.

Click here to instantly download the Use Case [PDF].

Click here for a full list of Use Cases that are also available for download.