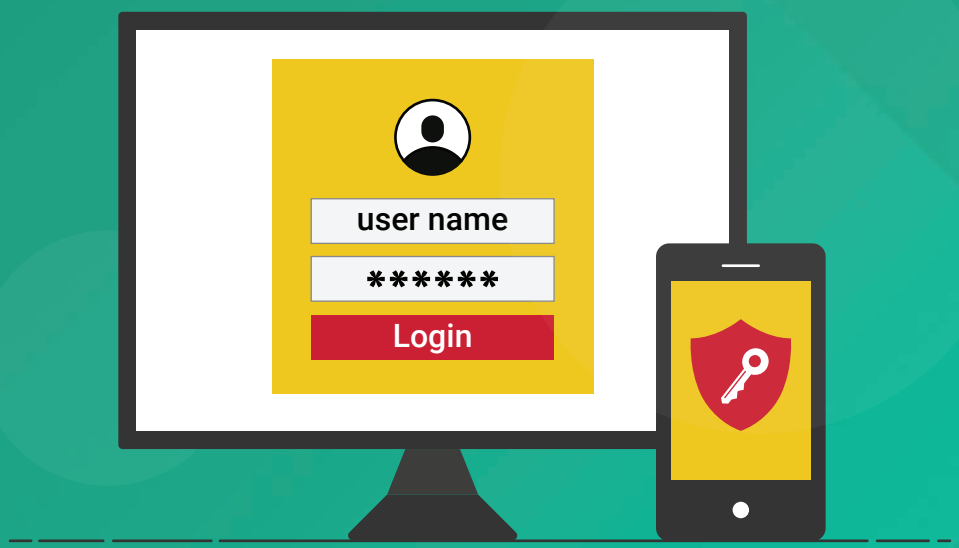
ManageEngine
ADSelfService Plus

Two-factor authentication for enterprise applications.

Double up on identity security.



www.adselfserviceplus.com

Introduction

Although information technology has come a long way over the past couple decades, the digital identities of employees are still protected by a simple username-password combination. For each application employees use, an additional username and password is added to the list of credentials employees have to remember. In fact, a 2017 survey by Digital Guardian revealed that more than 70 percent of their 999 participants had over 10 passwords to remember. To keep up, employees either use the same password for multiple applications, or resort to unsafe password storage methods with no regard to the security vulnerabilities they can cause.

Traditional authentication methods are not enough

To overcome the password fatigue employees feel when having to remember so many passwords, employees often:

- **Set weak passwords.**
- **Use the same password across multiple applications.**
- **Share their passwords with their colleagues.**
- **Write down all their usernames and passwords.**

IT administrators can't completely mitigate every poor decision users make, and these unsafe practices can easily put sensitive credentials in the wrong hands.

Since the traditional login method authenticates users using only a username-password pair, any person with these credentials can gain access. This method doesn't discriminate between employees or hackers, meaning it's no longer a secure way of authenticating users.

Two-factor authentication (TFA) and how it works

To differentiate between users and hackers, new additional authentication filters need to be added. One way to do this is by employing TFA. In this method, the user has to:

- **Enter something they know, like a username and password.**
- **Enter something they have or will receive, like an SMS or email-based verification code.**

A common scenario

These days, many online banking sites make use of TFA. First, the user logs into their banking portal using their username and password (something the user knows). In most cases, after the first successful authentication, the system sends a time-sensitive, single-use verification code to the user's registered mobile number or email (something the user has); in some cases, it may instead request another form of authentication, such as the corresponding account holder's debit card details. The user then enters the requested information to gain access to the system, thereby passing the second factor. The system validates the user if and only if the user correctly enters both the first and the second factor of authentication.

The right way to implement TFA

Although the implementation of TFA seems simple, there's a catch. A modern day tech user seldom uses just one application. With a higher number of applications often used, the user has to deal with the burden of entering credentials into each application separately. Suppose an employee uses five TFA protected applications for work. This employee has to enter ten different credentials (five username-password combinations and five verification codes) to access their applications. Constantly switching between usernames and passwords may lead to employees mixing them up and getting locked out of applications due to too many failed login attempts. Although most TFA solutions don't traditionally provide single sign-on (SSO), it's a great advantage if it does. This way, end users can access their enterprise applications after facing two-factor authentication just once instead of individually for each application.

Double up on security with the right tool

ManageEngine ADSelfService Plus is an integrated Active Directory (AD) self-service password management and SSO solution that offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications along with two-factor authentication.

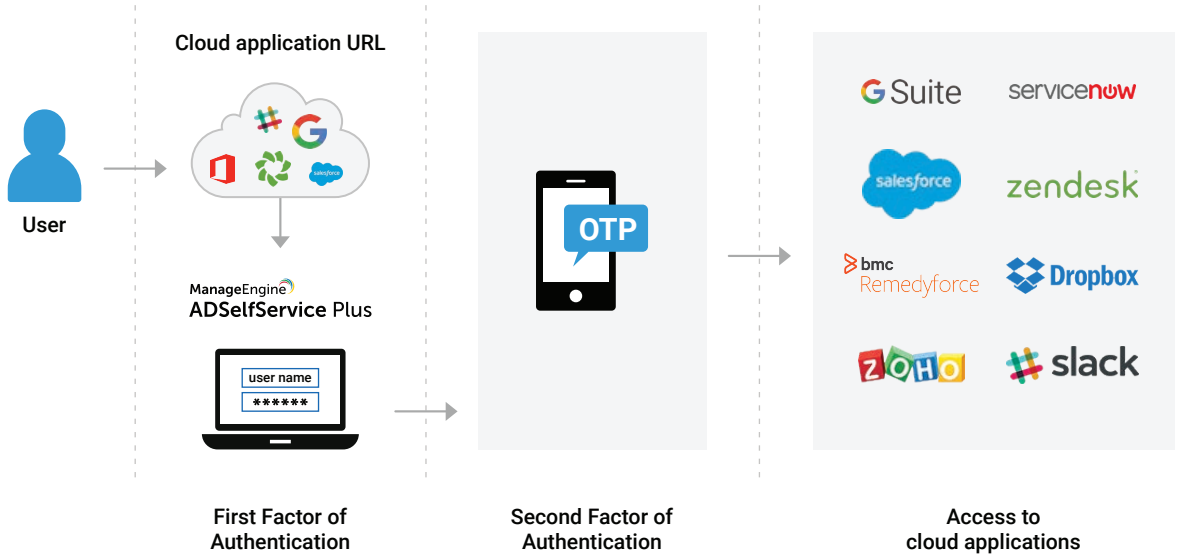
This solution provides TFA for many enterprise applications like Salesforce, Office 365, and Slack. Since TFA is provided as part of the service provider (SP)-initiated SSO (for SP supported applications), users can access all the configured enterprise applications after just one authentication process.

How TFA works in ADSelfService Plus

Prerequisites:

- **Users must be enrolled in ADSelfService Plus.**
- **The SMS or email servers must be configured properly in ADSelfService Plus.**
- **The user should have sufficient privileges from the self-service policies in ADSelfService Plus to use service provider (SP)-initiated single sign-on with TFA.**

Steps for users to enable TFA:



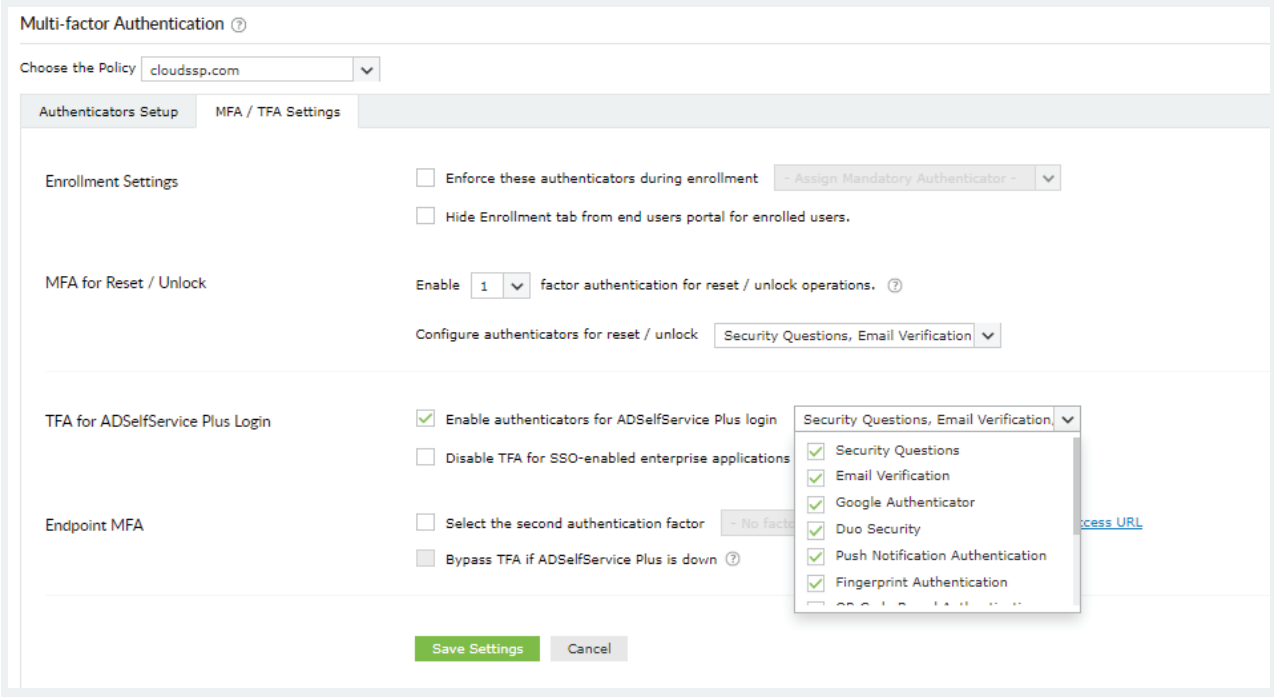
- Users must first access their cloud application by entering its URL directly into a web browser. The cloud application will redirect the user to the ADSelfService Plus login page for authentication.
- Users will need to enter their AD domain credentials to prove their identity.
- Next, users must authenticate themselves using the time-sensitive verification code sent to their registered mobile numbers or email.
- The user is now directly logged into the SSO-enabled cloud application and can also access all the other cloud applications to which they have privilege.

Advantages of using ADSelfService Plus as a TFA provider:

- TFA-based on OU/group memberships.
- SSO capabilities.
- Different password complexity rules for the first factor of authentication.

How to enable TFA in ADSelfService Plus in three, easy steps:

1. Log in to the ADSelfService Plus console as an administrator and navigate to the **Configuration** tab > **Multi-factor Authentication**.
2. Go to the **MFA/TFA Settings**.
3. Click the **TFA for ADSelfService Plus Login** option and select the required authentication techniques accordingly.



Once you've completed the above steps, TFA through ADSelfService Plus for all users falling within the selected self-service policy has now been enabled.