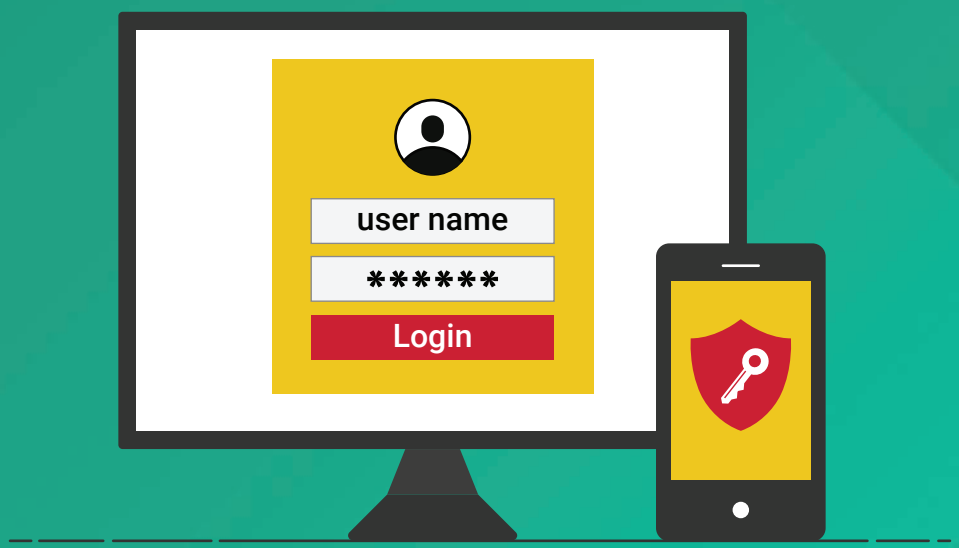
ManageEngine
ADSelfService Plus

Double up on security for Active Directory and cloud app authentication



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 site make use of TFA. First, the user logs in to 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). 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 implementing TFA may seem simple, there's a catch. A modern-day tech user seldom uses just one application. Since they often use many applications, users have to deal with the burden of entering credentials into each application separately. Constantly switching between applications may lead to employees mixing up their usernames and passwords, causing them to be locked out those 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. With SSO, end users can access each of their enterprise applications with just one set of credentials.

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.

Implementing TFA with ADSelfService Plus

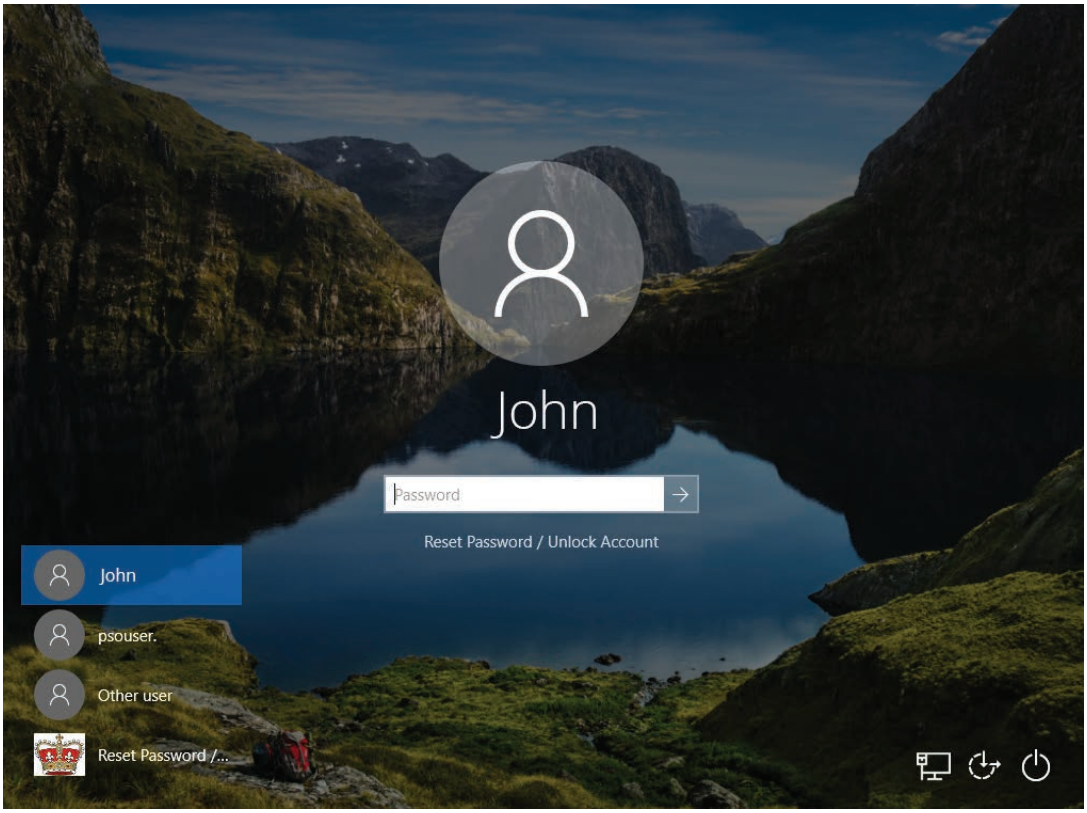
ADSelfService Plus supports TFA for logging on to Windows and applications. Although both logons are similar in functionality, the implementation process for each is slightly different.

TFA for Windows logon

With ADSelfService Plus, you can enable TFA for local interactive logons and remote desktop logons to both Windows clients and server machines.

TFA for Windows logon is supported by popular authentication methods, like:

- Duo Security
- RSA SecurID
- RADIUS
- SMS and email-based verification codes

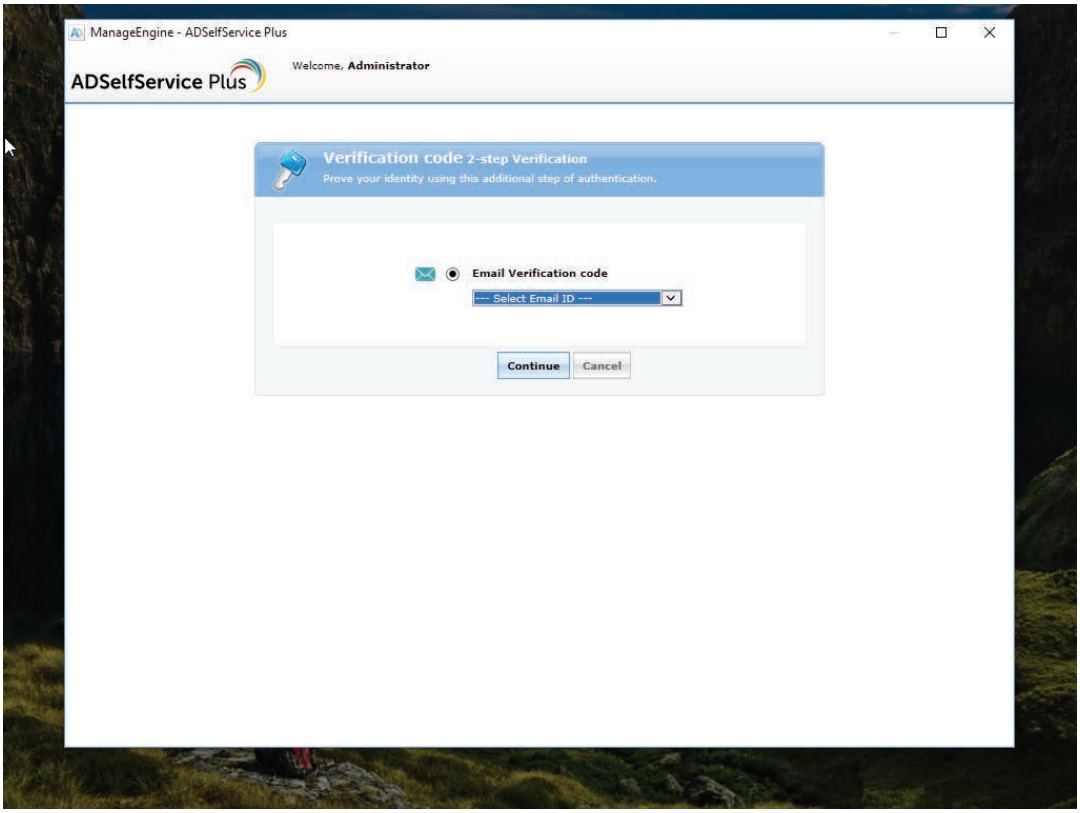


Prerequisites

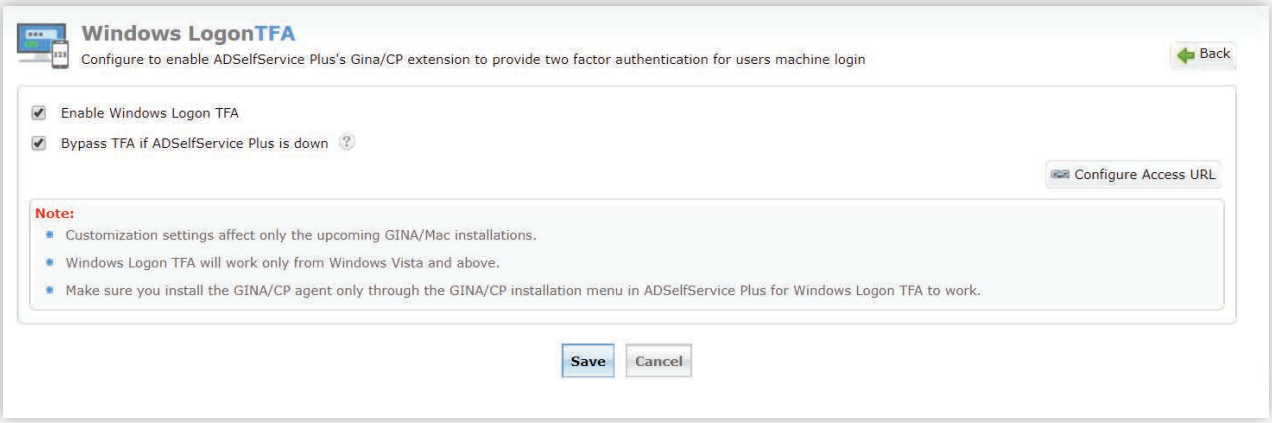
- SSL must be enabled.
- TFA must be enabled.
- GINA/CP client software must be installed on client machines. Make sure that the client software is installed through the GINA/Mac installation console.

Using TFA for Windows logon

- A user enters their credentials into the Windows logon screen as they normally would.
- Then, they receive the second form of authentication that has been configured for that user.
- Once they enter their authentication code, they'll be able to access their system.



Configuring TFA for Windows logon



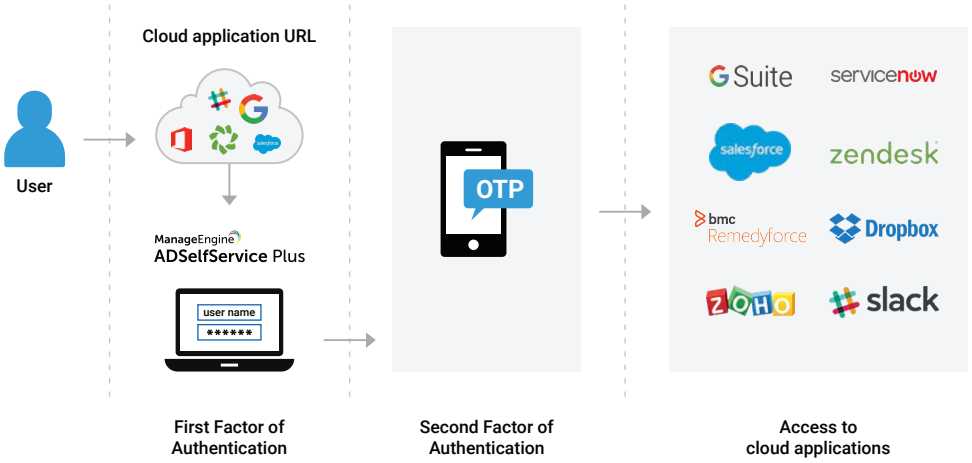
- Navigate to **Configuration > Administrative Tools > GINA/Mac** (Ctrl+Alt+Del) > **Windows Logon TFA.**
- Select the Enable **Windows Logon TFA** checkbox.
- By default, the **Bypass TFA if ADSelfService Plus is down** checkbox is selected when you enable Windows Logon TFA. If this option is left unchecked, users won't be able to access their machine when ADSelfService Plus is inaccessible.
- Check the settings under Configure Access URL to make sure that HTTPS is selected in the access URL.
- Click **Save.**

TFA for enterprise application login

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 SP-initiated SSO with TFA.

Using TFA for enterprise application login

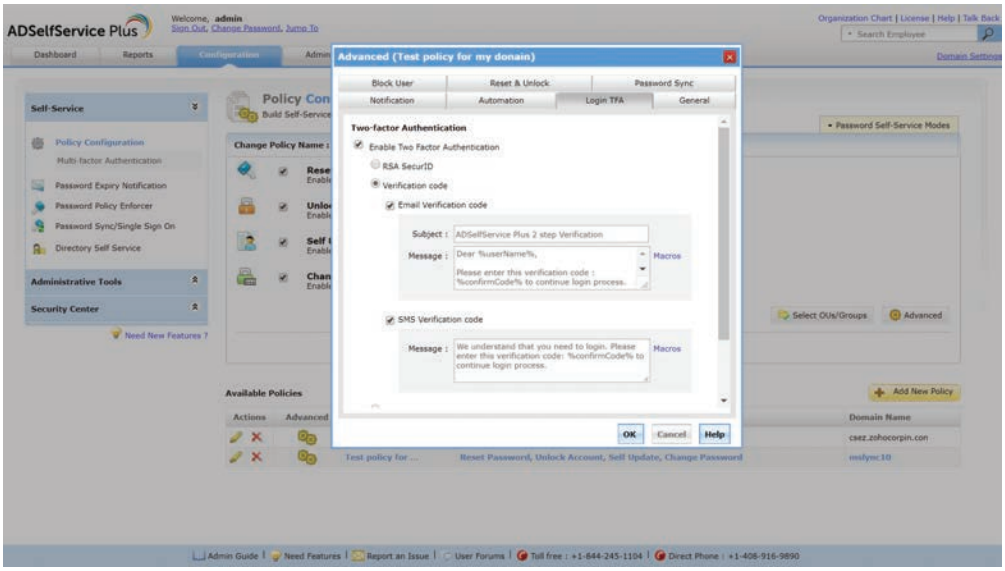


When users access one of their cloud apps through a normal browser:

- If TFA is enabled for that app through ADSelfService Plus, then they'll be automatically redirected to the ADSelfService Plus login page for authentication.
- From there, users need to enter their AD domain credentials to prove their identity.
- Next, users must authenticate themselves using a second form of authentication, like a one-time passcode.
- They'll now be directly logged in to the SSO-enabled cloud application and will also be able to access all the other cloud applications they have privilege to.

Configuring TFA for applications in three, easy steps

1. Log in to the **ADSelfService Plus console** as an administrator and navigate to **Configuration > Policy Configuration.**
2. Click the **Advanced** option and navigate to the **Login TFA** tab and check **Enable Two-Factor Authentication.**
3. Select the **Verification code** radio button and configure email and SMS servers accordingly.



Once you've completed the above steps, TFA through ADSelfService Plus for all users in the selected self-service policy will be enabled.

Advantages of using ADSelfService Plus as a TFA provider

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

ManageEngine
ADSelfService Plus

ADSelfService Plus is an integrated Active Directory self-service password management and SSO solution. It offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and SSO for cloud applications. ADSelfService Plus supports IT help desks by reducing password reset tickets and spares end users the frustration caused by downtime.

For more information, please visit www.manageengine.com/products/self-service-password.

$ Get Quote ⬇ Download