AT&T Business

Secure access to your corporate network and prevent identify fraud with AT&T Multi-Factor Authenticator

The AT&T Cybersecurity Consulting team has been providing **industry-leading security solutions** for over 25 years.

The majority of data breaches are caused by brute force attacks on credentials. We use the powerful FIDO2 (Fast Identity Online) authentication standards to prevent unauthorized access to your network and help keep your business safe.*

AT&T Business wants to make sure you have the latest protections in place to help keep your data, your reputation, and your business safe and secure. AT&T Multi-Factor Authenticator (AT&T MFA) uses next generation security protocols available to protect your network and devices from breaches related to identity.

False sense of security

You might already have some type of multi-factor authentication as an additional login security layer. But did you know that many of today's solutions have significant security flaws? Current two-factor authentication is easy to manipulate. Cybercriminals use automated code breaking brute force attacks to infiltrate a network, steal passwords, and steal or ransom your data or your customers' data. It's more difficult and costly to clean up after an attack than to prevent it in the first place. To stay ahead on security, it's a smart move to invest in a virtually unphishable credential authentication system.

Benefits

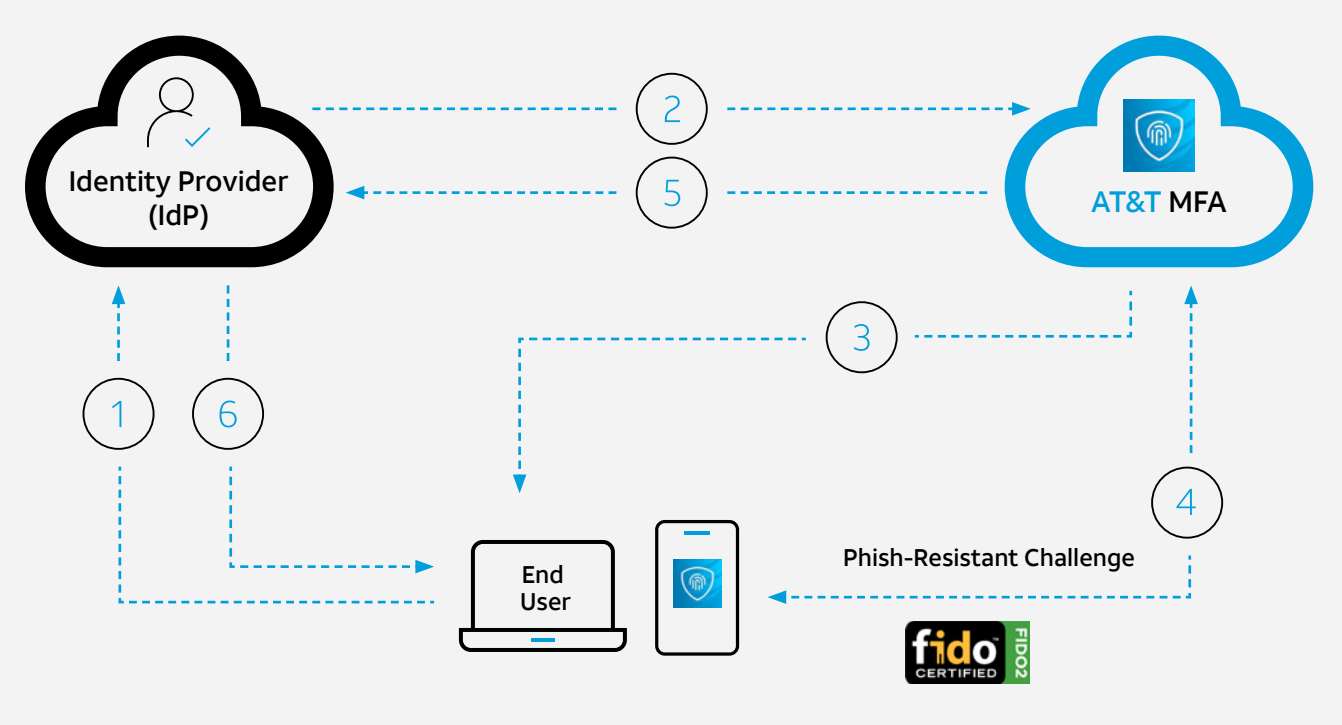
- **Highest level of security:** Features Fast Identity Online (FIDO2), among the strongest authentication standards available
- **Zero trust security:** Trust no one, authenticate everyone, internal or external
- **Increase security, not hardware:** Multi-Factor Authenticator is phish-resistant with end-to-end cryptography through our smart phone application
- **Lower cost of ownership:** Uses existing smartphone and AT&T MFA app - no physical security keys or hardware needed
- **Rapid deployment:** No delays from purchasing and distributing physical security keys or hardware
- **Easy-to-use** smartphone app with familiar push notifications

Zero trust for the latest protection

AT&T MFA is a next-generation FIDO2 solution that features a phish-resistant authentication factor, secured by cryptography. The service leverages a smartphone application in place of a physical security key, solving the challenges that frequently prevent enterprises from implementing FIDO2 MFA. It can be quickly and easily deployed using an existing smartphone, eliminating the need for costly and cumbersome hardware security keys that could be lost or stolen and provides the highest level of authentication security with a frictionless user experience. AT&T MFA reduces the risk of phishing and supports the eventual evolution to the passwordless future of authentication.

Plus, you can activate and manage AT&T MFA in our customer portal. The portal enables you to conveniently monitor activity and performance. AT&T MFA integrates with AT&T Enterprise Application Access, AT&T Enterprise Traffic Protector and other cybersecurity platforms to enforce a zero-trust network protocol in which all users, whether they are internal or external, must be authenticated.

How it works:



1. The User provides their username and password to the directory/primary authenticator (e.g.,Microsoft Azure AD).
2. When the username and password are validated, the primary authenticator connects to AT&T MFA to generate the second factor.
3. AT&T MFA renders a page for the user to select an authentication factor.
4. AT&T MFA sends a challenge - the phish-proof push - to the user's smartphone and receives a response from the user.
5. Once the response is received, AT&T MFA passes control back to the primary authenticator.
6. The primary authenticator then allows the user to proceed to the request application of service.

AT&T Business

AT&T MFA features:

- **Phish-resistant:** FIDO2 security provides the highest level of security using an easy and familiar application push notification.
- **Configurable and customizable:** Select the authentication method you need to fit your needs, including phish-resistant push, standard push, Time-based One-time Password (TOTP), and SMS (short message service, or texting).
- **Compatible with existing authentication technologies**: Includes magic link email or text, voice call, biometrics, and more.
- **IdP integration:** Easily integrate with market-leading identity providers (IdP) and identity solutions such as Microsoft Azure and Okta to provide a seamless service.
- **Automated provisioning:** Using System for Cross-domain Identity Management (SCIM) ensures changes in your directory are reflected immediately.
- **Authentication event reporting**: A complete set of rich reporting features keeps your administration team informed of authentication events and ensures users comply with network protocols.
- **Controlled or self-service user enrollment**: We offer a variety of easy-to-use methods for enrolling end users and registering devices to reduce the workload on administrators while meeting requirements in your business policies.
- **Global reach and scale:** Ensures resilience and performance world wide.

Why AT&T

Cybersecurity is complex. The threat landscape changes fast. It can be difficult to know you're making the right security choices. We reduce the complexity and cost of fighting cybercrime while enhancing the speed and strength of your response to network threats.

To learn more, contact your AT&T Business representative or visit the AT&T Business website: **https://aem-preprodbusiness.test-e.att.com/products/multi-factor-authenticator.html**

*https://fidoalliance.org/fido2/

[1] ID Agent, "10 Game-Changing 2020 Data Breach Statistics," July, 2020