AT&T Business

Help protect data, networks, and applications through enhanced and flexible security

Description

As companies open their networks to a wide variety of remote users such as mobile employees, customers, partners, resellers, and suppliers, they risk the exposure of highly valuable, proprietary, and sensitive information.

To better protect their information, many companies are taking stronger steps to authenticate who is authorized to access their network resources. These steps protect their data by controlling who gets access to specific resources and incorporates centralized and automated policy management to match their security posture.

AT&T Token Authentication Service is a cloud-based, highly flexible user authentication service that helps control access to your network, applications, and sensitive data to reduce those risks. It provides enhanced access security for a wide range of customer applications ranging from enabling stronger authentication for a Virtual Private Network (VPN) to enforcing highly secure access across an entire enterprise.

It uses Multi-Factor Authentication to provide stronger and more reliable user authentication than single-factor passwords or personal identification number (PINs). This service provides automated provisioning and management, with a flexible policy management approach that lets you specify blanket definitions combined with highly granular policy options. Predefined best-practice security policies are offered based on roles and delegation rights that can be fully customized.

The service is easy to implement and manage. You can deploy the AT&T Token Authentication Service quickly with low total cost of ownership because it requires no installed equipment at your premises. The service includes a user-friendly portal for complete administration. AT&T Business also provides 24x7 customer trouble support to provide you a variety of service options to meet the unique needs of your business.

Key needs met

Security – Help protect sensitive data and resources vital to the organization. Safeguard your business with enhanced security when users access your network, company resources, and information systems – especially mobile users who access cloud services.

Access – Gain and maintain access controls to the vital information and communications resources needed for your business. A user authentication service that's both easy to manage and provides useful information about usage gives you the control you need.

Prevent data and identity theft – You need strong yet flexible identity authentication controls – the best prevention method against thefts, which also help ensure business continuity.

Meet regulatory and compliance requirements – Stay on top of these ever-changing requirements whether they're related to access, personnel, customer data, or proprietary data.

Control costs – With reduced reliance on passwords, AT&T Token Authentication Service helps control costs like calls to a helpdesk. The cloud-based service requires no on premises equipment or a monthly pay-per-user model, regardless of the number of applications.

How it works

To use AT&T Token Authentication Service, you issue hard or soft tokens to users who then access the service via the internet (internet access is required). A user with a token can enter an ID and passcode comprising a PIN and a token generated code. The service authenticates the user ID and passcode. The Token Authentication service uses a Hardware Secure Module (HSM) that complies with FIPS 140-2 Level 3 and resists attack vectors. After authentication, the service allows the user to access apps using a desktop or laptop computer (Windows® and Mac®) or a mobile device (iOS®, Android™, and Windows®). In addition, an administrative portal enables you to centrally manage policy and configuration at the group or user level and establish an audit trail.

Features and benefits

- Enhanced security offers protection across your entire deployment, covering remote access servers, VPNs, web portals, enterprise networks, and cloud-based applications
- Multi-Factor Authentication (MFA) to help reduce the risk of unauthorized access
- Flexible policy management provides centralized control with granular policy controls to protect your network where you need it most; includes a flexible, risks-based access policy matching your login environment and single sign-on (SSO) to streamline navigation processes through your cloud applications Connectivity Management
- Simplified management with automated provisioning, administration, active directory synchronizations for easier implementations, and potential reductions in total cost of ownership
- Mobile Authenticator App: Mobile PASS+ applies protection at enrollment in addition to end-to-end encryption
- Supports major operating systems: Apple iOS, Android, Chrome OS and Windows 10 or 11
- Simplified integration with hundreds of cloud applications and compatibility with hybrid applications, VPN gateways, virtualization solutions, or on-premise solutions

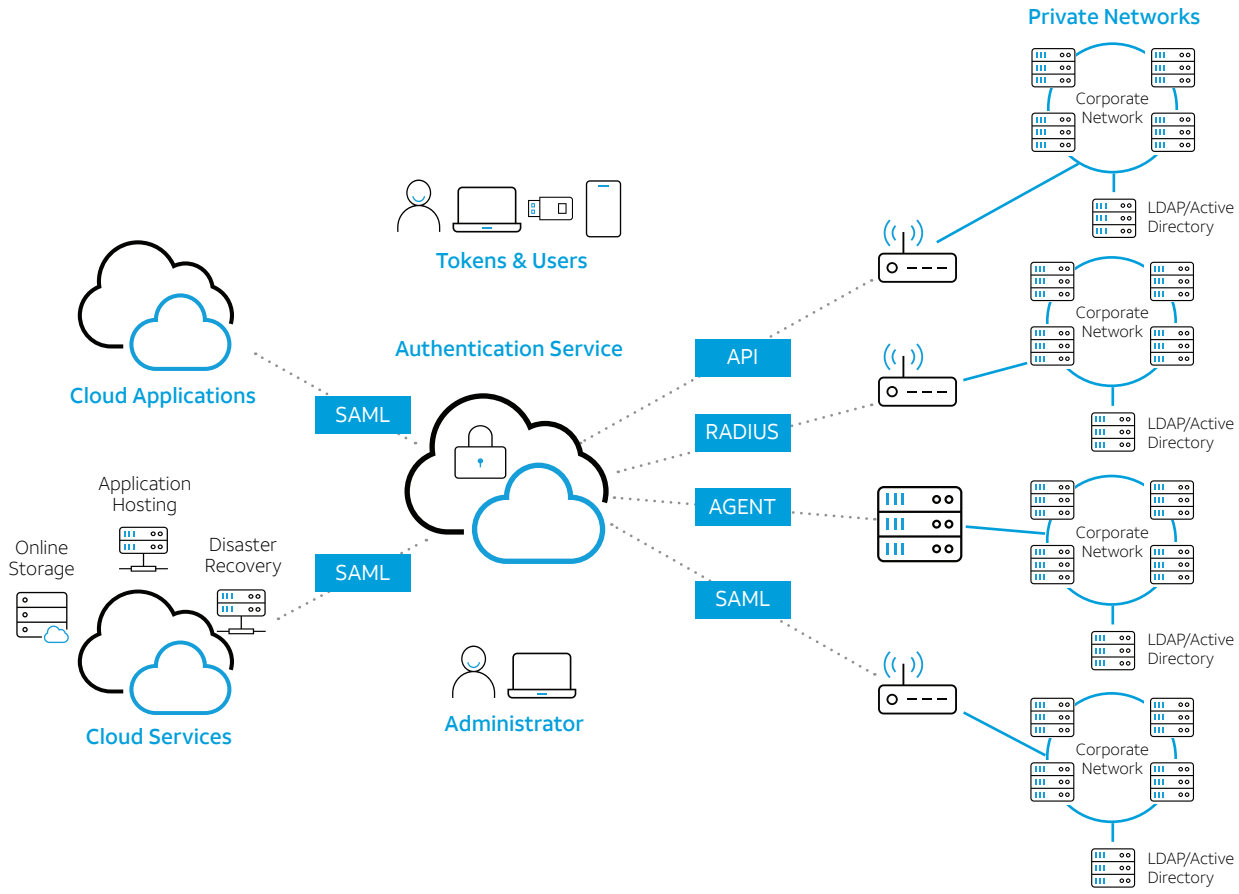
Information Security

Every organization has daily challenges to solve to provide the best for its customers while also protecting the business. In addition to managing rising administrative and operating costs, you must provide employees, customers, suppliers, or even regulators with access to electronic records. And to protect privacy, you may also have compliance requirements. Health Insurance Portability and Accountability Act (HIPAA) requirements are one example. To help secure sensitive information without adding to your administrative burdens, we suggest user authentication using AT&T Token Authentication Service.

In addition, we support the security features with our technical expertise, management, customer care, and provisioning services. AT&T Business provides a comprehensive solution that helps you reduce capital expenditures and staffing and maintenance expenses. And because of its strong security features, it may also capably support your compliance program.

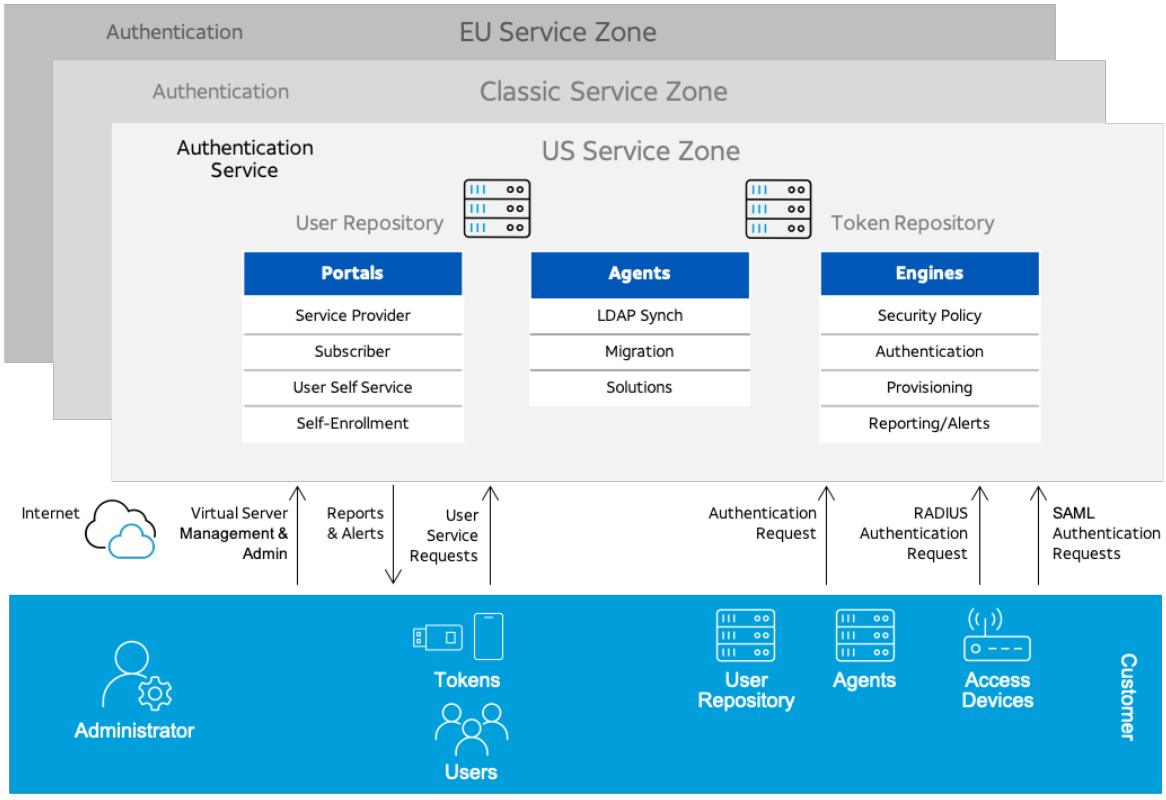
AT&T Token Authentication Service – Deployment architecture

This diagram depicts a typical use case scenario in which the service authorizes user access via data on authentication servers and RADIUS and SAML protocols.



AT&T Token Authentication Service – Technical design

This diagram provides an overview of how the different service components work together to provide user authentication.



AT&T Business advantages

- **Data Network Strength –** AT&T Business understands data transportation and networks. We own and operate wireline, wireless, and IP data networks, including one of the world's most advanced and powerful IP backbones. Our networks offer local, national, and global coverage. With our expertise in data networking and access management, we're able to provide dependable authentication services so that you can focus on your business.
- **Security –** AT&T Business has one of the most comprehensive cybersecurity portfolios in the industry. We build in robust security measures at every network layer to help reduce the risk of outages and intrusions. We take advantage of our extensive experience in this area to design a reliable and highly secure token authentication service for you.
- **Service –** We offer you easy access to self-service options and expert support, whether through online tools or a single phone number. As a result, you may spend less time on service issues and have more time to focus on your organization. AT&T Business provides white glove onboarding, training for your administrators, and 24x7 customer trouble support.

For more information, contact your AT&T Business representative or att.com/security.