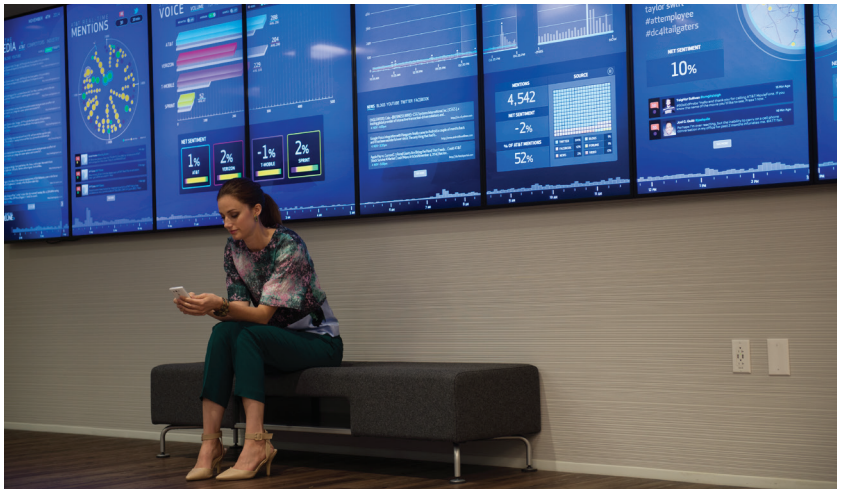
AT&T Business

Help protect data and applications through enhanced security



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.

As a result, organizations are taking a stronger stand regarding authenticating authorized users of their network resources – protecting their data assets by controlling who gets access to specific resources and incorporating centralized and automated policy management to match their security posture.

AT&T Token Authentication Service – provides enhanced access security for a wide range of customer applications ranging from enabling stronger authentication for a Virtual Private Network to enforcing highly secure access across an entire enterprise. It 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.

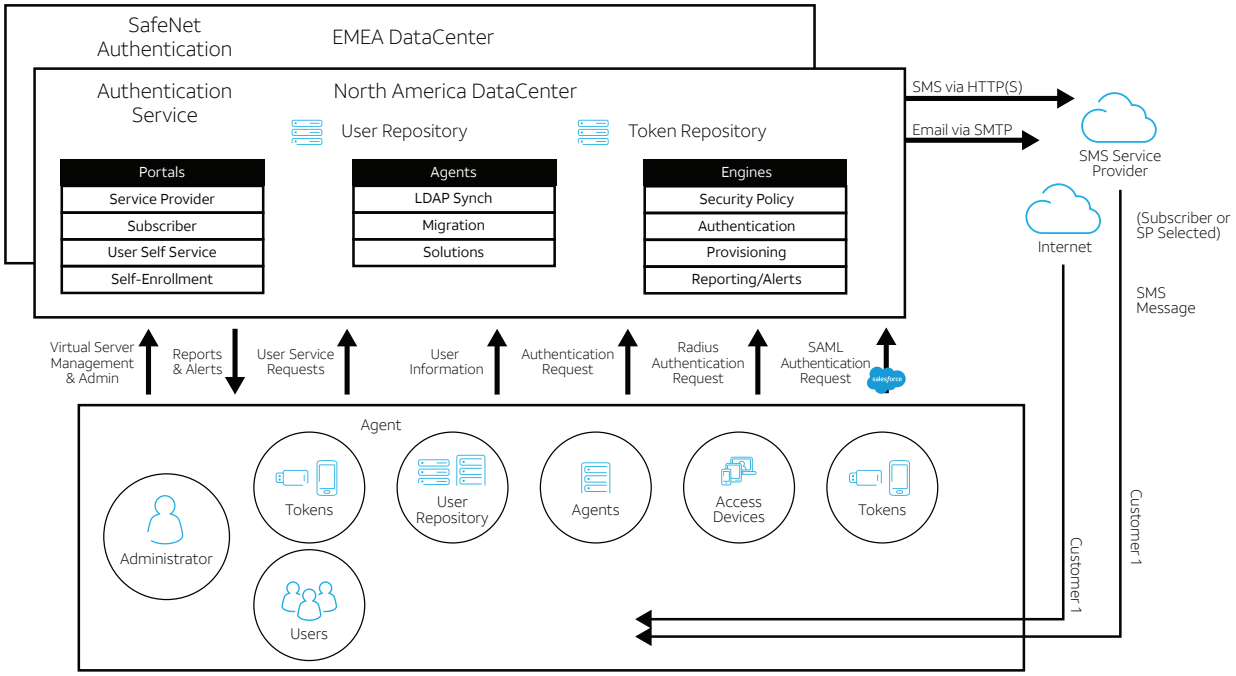
Potential Benefits

- Enhanced security offers protection across your entire deployment, covering remote access servers, VPNs, Web portals, enterprise networks, and cloud- based applications
- Flexible Policy Management provides centralized control with granular policy controls to protect your network where you need it most
- Simplified Management with automated provisioning, administration, and service management for easier implementations and potential reductions in total cost of ownership

Features

- Two-factor authentication to help reduce the risk of unauthorized access
- Multiple Token Authenticators – Key Fob or various software authenticators
- Supports major mobile platforms: Apple iOS, Android, Windows Mobile, and Blackberry

AT&T Token Authentication Service



Service Description

The AT&T two-factor authentication approach requires a user to provide two unique factors: something they know, like a password or PIN, and something they possess like an authenticator, a hardware or software token with a code that changes randomly every sixty seconds.

This two-factor authentication makes it far more difficult for a hacker to gain access to authentication credentials. AT&T Token Authentication Service is supported by state-of-the-art Data Centers, providing fully redundant and fully diverse network access.

Our managed token authentication service is a multi-tenant/multi-tier infrastructure that offers 99.999% service availability and is supported in highly secured data centers, staffed with security professionals 24x7.

Let us help you protect your network against unauthorized access and the losses associated with network security breaches by implementing our Token Authentication Service in concert with your overall Security Policy.

For more information contact your AT&T Representative or visit us at www.att.com/authentication.

To learn more about AT&T Token Authentication Services, visit www.att.com/authentication **or** have us contact you.

Share this with your peers