WaTech
Washington Technology Solutions

Strong Authentication

Last updated 2-28-23

WaTech's Strong Authentication service verifies user identity with a two-part authentication process. It uses one item users know—a PIN—and one item that users have—a token—to provide a one-time password. This provides a much stronger and more reliable level of authentication than a password.

This service can be used to verify the identity of users who access a variety of agency applications or resources, such as:

- Web applications.
- Wireless access points.
- Routers and switches.
- Virtual private networks (VPNs).

Intended customers

Intended users of this service include members of the Enterprise Active Directory (EAD) and organizations with a Master Service Agreement (MSA). Other intended customers include organizations that are connected to the State Government Network (SGN) and agencies that are part of WaTech's Small Agency IT Service and external organizations such as tribes, national parks, cities or counties.

Options available with this service

- Software Token available on Windows, iPhone, Android operating systems.

Customer engagement

- Semi-annual customer Town Halls with all Network Services teams providing updates and gathering customer feedback.
- Monthly Technology Management Council meeting for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy, and investments.
- Regularly scheduled meetings between customers and Business Relationship Managers to connect, advise, address concerns and provide solutions.
- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives, and services.
- Requests for new consultations and modifications to existing applications.

Action plan

Current Activity
Integrating this service into the Network Services Division (NSD). This service integration will enable a more streamlined and straightforward response to customer questions as well as standardized troubleshooting processes.

One- to two-year goals
- Develop a comprehensive Secure Service Edge (SSE) Strategy as part of a Secure Access Service Edge (SASE) Framework, which will

Helpful information

Service category
Network

Service availability
24/7/365

Planned maintenance
Planned maintenance is performed after hours and coordinated with agency representatives.
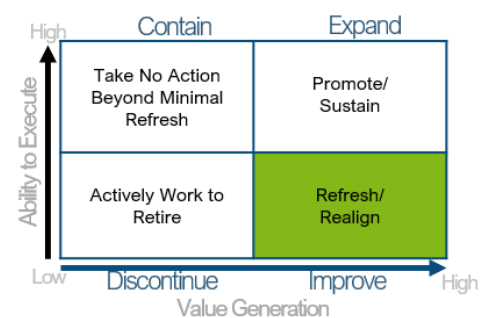
Related services
- Virtual Private Network (VPN)
- Azure Active Directory w/MFA

How to request service
Submit a request for service through WaTech's Customer Portal.

Service owner
Jason Miller

influence (dictate) the evolution of this service. Once WaTech finalizes its SASE Blueprint, WaTech will leverage the Systems Engineering Framework to determine how this service will evolve as a lifecycle plan is developed.

Three- to five-year goals

WaTech will evolve this service based on an approved lifecycle plan as part of WaTech's SASE Blueprint in alignment with the WaTech Strategic Roadmap, the state's Strategy Map, and legislative intent (as declared in House Bill 1274).

	Jan	2023	Dec	Jan	2024	Dec
Strong Authentication		SSE Strategy (summer 2023)	F5 Architectural Lifecycle Plan (fall 2023)		Service Action Plan updated & Service Evolution begins.	

Service review and fully loaded service budget projection

The strong authentication service is a fee-for-service rate structure. Revenue received from this service is reincorporated directly back to the service for equipment refresh and administrative support. The Remote Access cost center includes strong authentication service as well as SSL Virtual Privat Network (VPN) service.

Due to the COVID pandemic and the number of state employees working remotely, revenues for this service increased substantially in last three years. WaTech is exploring a new service delivery model to modernize the service which will likely require new investments. In FY 22, WaTech worked with customer agencies to transition from hardware token authentication ($17.45 per user per month) to other methods of authentication ($6-$9 per user per month). The number of hardware token users went from 943 in July 2021 to 85 in June 2022.

Cost Center 3541 | Remote Access Services