

## SecureAccess Washington (SAW)

Last updated 01-25-23

[SecureAccess Washington](#) provides self-administered single sign-on access to hundreds of agency applications, shields online services from harmful activity, and allows access only to authenticated users.

To use a service or application protected by SecureAccess Washington, you must provide a user ID and password. The agency owner of the service is responsible for allowing or denying access and for verifying individuals' identities.

Some agencies use SecureAccess Washington to provide selective access to their online documents or services. Examples of these documents and services include Paid Family Medical Leave, SEBB MyAccount, and Driver License Renewals.

SecureAccess Washington provides an uptime target of 99.7%, which is always met; actual uptime is closer to 99.9%. Agency customer requests are responded to within one business day; agency requests for enhancement are reviewed for quarterly user interface builds. A minimum of four major releases per year are created to provide ongoing usability improvements. Emergent requests from agency customers are triaged by a 24/7 on-call rotation of subject matter experts. The WaTech Support Center responds to resident requests Monday through Friday during business hours (6am-8pm). Monitoring of the Monday-Friday ticket creation for the month of December indicated that about 10% of SecureAccess Washington's tickets came in outside of core business hours. Tickets submitted on Saturday and Sunday accounted for an additional 11%.

### Intended customers

Intended customers are agencies that are part of the Secure Gateway Services allocation. WaTech OCIO Policy 141.10 requires the use of SecureAccess Washington for single sign-on authentication for resident users. SecureAccess Washington provides reverse proxy services to agencies hosting applications on the SGN and offers SAML 2.0 integration capabilities to cloud-hosted agency applications. SecureAccess Washington currently provides access to more than 300 state services to resident users at any given time, and the SAW team is working to onboard 10-12 new services to the single sign-on portal. The customer base is expected to grow once SAW adopts OpenID Connect integration capabilities and new identity verification processes. OpenID Connect is an additional integration option sought by several customers by 2024. SAW Currently supports legacy integrations with on-premises applications and SAML 2.0 integrations for cloud-hosted agency applications.

### Options available with this service

- LexisNexis Knowledge based authentication is available as an add-on fee for service. This service provides a one-time identification of a user based on name and address via three to five question public records quiz.
- Professional services are also available to onboarding customers that require additional business analysis or technical help.

### Customer engagement

- The Secure Gateways Team holds a biweekly [Secure Gateway Services Fireside Chat](#).
- The SecureAccess Washington Technical and Business Advisory Group holds meetings on an ad-hoc basis.

## Helpful information

### Service category

Security

### Service availability

24/7/365

### Planned maintenance

Performed as required during non-peak hours. The third Tuesday of each month from 5:30-7:30 a.m. is reserved for routine maintenance activities.

### Related services

- [Fortress Anonymous](#)
- [WA.gov](#)

### How to request service

Submit a request for service through our [Customer Portal](#).

### Service owner

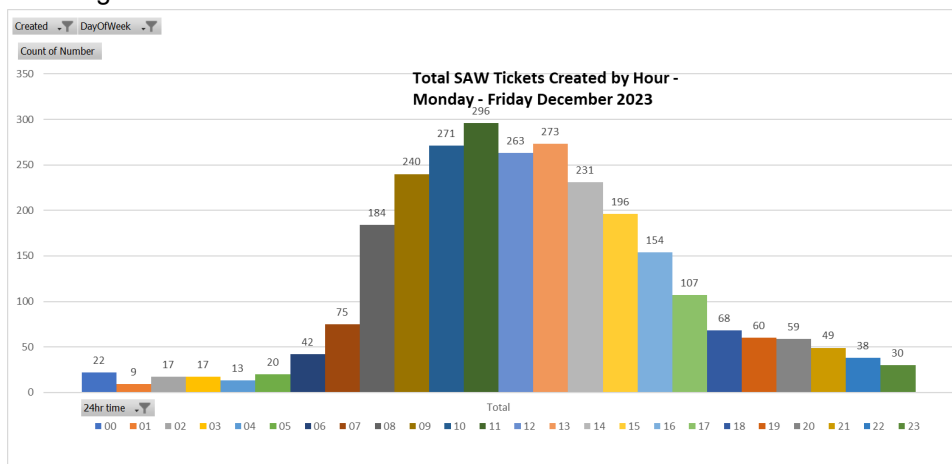
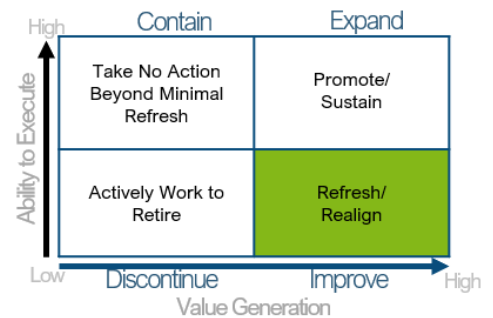
Audrey Leckner

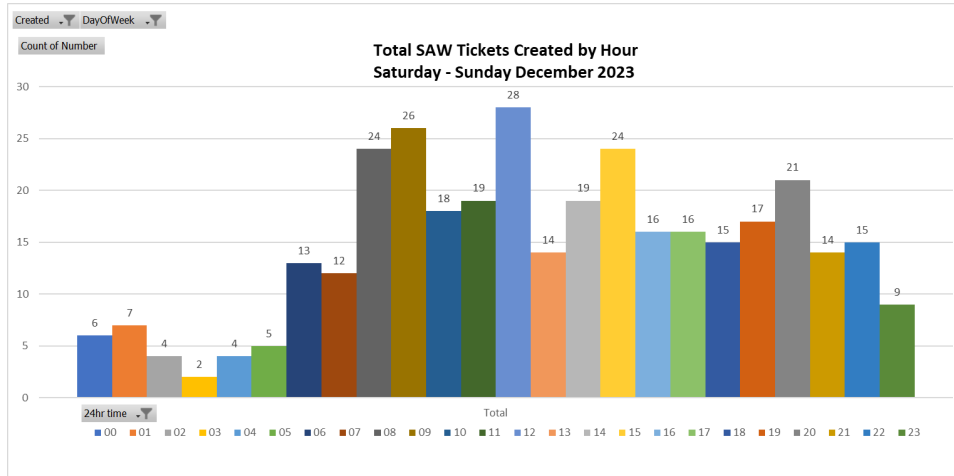
- Semi-annual customer Town Hall with all Computing Services teams providing updates and gathering customer feedback.
- Monthly Technology Management Council (TMC) and Business Management Council (BMC) meetings for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- Regularly scheduled meetings between customers and Business Relationship Managers (BRM) 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

- SecureAccess Washington recently introduced chat services to the login portal to answer frequently asked questions. In addition, Twitter has been added to the portal to provide timely updates regarding the service.
- Requirements have also been gathered for a replacement to the Identity Verification solution provided at SAW, as well as a refresh of the SAW Administrative user interface.
- Full Spanish translations and chatbot support will be released in the Q1 2023 SAW Build
- Monthly metrics including uptime, number of applications served, number of agencies onboarded, number of unique and total logins per month, and number of support tickets served by WaTech shared at Bi-weekly customer meeting. New metrics to determine success of single sign-on efforts and ability to receive, triage, and deliver SAW enhancements under development.
- Monday-Friday ticket creation for the month of December indicates that about 10% of SecureAccess Washington’s tickets come in outside of core business hours.





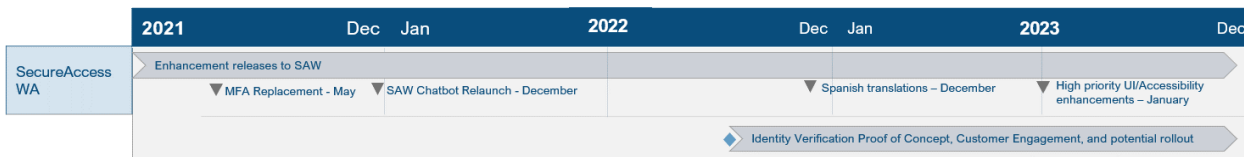
**One- to two-year goals**

- Project underway to provide full Spanish translation to SecureAccess Washington as well as two new usability studies and builds to address customer friction at the portal.
- Replacement or addition to LexisNexis KBA or user identification.

**Three- to five-year goals**

The following items have been identified outside of the Resident Identity and Access Management strategy, for development. If the IAM projects are funded, these may change or become adopted into that program, as specific software builds for a legacy system may not be prioritized.

- Provide integration capabilities via OpenID Connect as a new integration method.
- Preparing to restructure the service to better support integrations with commercial off the shelf (COTS) systems.
- Chat services will be expanded on a continual basis to address authentication issues, as well as further integration with agency-provided support desks to help route residents to the correct service desk for triage.
- Integrate the administrative user interface with the Enterprise Active Directory solution as the administrative functions are overhauled.



**Service review and fully loaded service budget projection**

**Revenue source:**

The SAW service is bundled and funded using revenue from the Security Gateway central service model.

The Security Gateway Allocation funds a central point of authentication for all public-facing services provided by Washington state agencies, which enforces security standards to protect state citizens’ private information when accessing government services. It provides a consistent method of authentication and should result in efficiencies/savings at the agency level with these services provided at the enterprise level.

Allocation funding is based on the agency’s number of budgeted FTEs and the number of applications each agency has using the gateway. OFM maintains the source data for budgeted FTEs and WaTech tracks the number of applications. Additionally, agencies with 50+ FTEs pay a yearly base fee of \$1,500.

**Net Income over time:**

