

Service Description

The OIT Secure Authentication service provides a managed two-factor user authentication solution to protect an agency's resource. The authentication function requires the user to identify themselves with two unique factors, something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to a customer's environment.

A Secure Authentication customer might also be interested in these OIT services:

- Ohio One Network

Customer Benefits

- **Cost-savings** – The customer will save money by not having to incur additional expenses for personnel and equipment associated with monitoring and maintaining the service.
- **Security** - This service offers protected exchanges of information to block unauthorized access.
- **Support** - Service support is provided by OIT staff that is skilled and experienced in planning and provisioning, maintaining, and troubleshooting the service.

OIT Provides

- Administration
- Authentication servers
- Incident resolution services via the Customer Service Center
- Licenses
- Routine maintenance
- Service monitoring and alerting
- Service provisioning and implementation

Maintenance Schedule

Scheduled maintenance occurs every Tuesday from 3:00 a.m. to 6:00 a.m. Outages will be minimized or canceled whenever possible. OIT schedules extended outages twice per year. The scheduled extended outage dates are negotiated with the customer at the beginning of the year, and typically run from 6:00 p.m. to midnight. If a shorter outage window is required, the outage will be scheduled from 6:00 p.m. to 9:00 p.m.

Incident Response & Resolution

As a primary service, Secure Authentication support staff is available 24 x 7 for both incident reporting and resolution. Secure Authentication staff will respond to the customer within 30 minutes of a reported incident. Customer involvement is essential to resolving issues; therefore, the customer will need to provide a Technical Contact resource. With collaboration from the customer and vendor resources, staff will commit to resolve the incident within 4 hours.

Service Objectives

Category	Evaluation Criteria	Target
Availability	Secure Authentication uptime	99%
Incident Responsiveness	Secure Authentication support staff responds to the customer (i.e. acknowledges and confirms receipt of incident ticket) within 30 minutes.	100%
Incident Resolution	Secure Authentication support staff resolves incident within 4 hours.	75%

Customer Requirements

- Account information for each token user
- Authentication tokens or Smart Phone application
- Configuration of agents to connect to OIT's authentication servers
- Maintain agency and service contact lists via the IT Enterprise Services portal at: <http://itenterprise.ohio.gov>.
- Place service order via the OIT Enterprise Service Catalog
- Provide DAS OIT with a valid billing number

Additional Information

For more information on this service contact the **Customer Service Center** at CSC@ohio.gov or visit the **IT Enterprise Services** portal to place an order at <http://itenterprise.ohio.gov>. Rate information for this service can be found on the [DAS OIT IT Business Office](#) site.