Ohio | Department of Administrative Services

Identity Management

Service Description

Identity Management provides integrated authentication services across multiple enterprise service offerings. The service also streamlines the life cycle events for user credentials including onboarding, provisioning, administration, service consumption, change events, de-provisioning and off-boarding.

Identity Management is made up of four service functions:

- **Identity Repository** offers a centralized container for all user credentials and management tools for the administration of those credentials and credential attributes.
- **Core Shared Services** leverage the centralized credential from the identity repository for authentication. Service provisioning tools are available to provision access to various portions of the core shared services within the Identity Management service.
- **Application Integration** permits an agency's line of business application to authenticate to the centralized user credential within the Identity Repository using a secure Lightweight Directory Access Protocol (LDAP) and/or Active Directory Federation (SAML 2.0)
- **Endpoint Consumption** allows for the placement of desktops, laptops, and/or tablets to reside within the Identity Management service. This extends the ability to use a single credential to authenticate to workstations and applications.

An Identity Management customer might also be interested in these OIT services:

- Email
- SharePoint
- Shared File Services

Customer Benefits

- **Availability** – This service has various levels of redundancy built in as part of its architecture.
- **Efficiency** – The provisioning and de-provisioning process is tied to the Ohio Administrative Knowledge System (OAKS) Human Capital Management (HCM) application so there is a single onboarding and off boarding process for consumers as opposed to a duplicate process for each core shared service.
- **Administration** – This service is built upon a delegated administrative model so agencies can still support their own management needs.
- **Support** - Service support is provided by staff skilled and experienced in planning and provisioning, as well as maintaining and troubleshooting the service.

OIT Provides

- A centralized and automated account credential provisioning/de-provisioning
- A single account credential for multiple core shared services
- An agency focused web portal for various management tasks
- A user self-service web portal for password reset
- Secure LDAP authentication services for agency line of business applications
- Incident resolution services via the Customer Service Center
- ADFS (SAML) authentication services for agency line of business applications

Maintenance Schedule

Scheduled maintenance of Identity Management occurs on Wednesday evenings from 6:00 p.m. to midnight when needed. Outages are minimized or canceled whenever possible. OIT schedules extended outages twice per year. The scheduled extended outage dates are established at the beginning of the year and typically run from 6:00 a.m. to midnight. If a shorter outage window is required, the outage will be scheduled from 6:00 p.m. to midnight.

As a primary service, Identity Management support staff is available 24 x 7 for both incident reporting and resolution. Identity Management 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.

Note: The customer is responsible for providing end-user support for this service.

Service Objectives

Category	Evaluation Criteria
Availability	Identity Management service uptime
Incident Responsiveness	Identity Management support staff responds to the customer (i.e. acknowledges and confirms receipt of incident ticket) within 30 minutes.
Incident Resolution	Identity Management support staff resolves incident within 4 hours

Customer Requirements

- An active State of Ohio User ID issued from the OAKS HCM application for both State and contingent workers
- 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

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.