IOT Identity & Access Management Team - 2023

Who We Are:

An 10 - member team that supports and maintains identity and access service technology infrastructure for all supported State agencies as well as their business partners and constituents.

Our Mission:

The IOT Enterprise Identity Services team works to provide enterprise grade authentication and access control needs to all State of Indiana supported Agencies and where applicable business partners and customers. Nearly every service or modern business process integrates with our Active Directory based infrastructure offerings. Therefore, we strive to increase productivity across platforms through modern SSO opportunities yet keep data and identities secure and highly available.

Located:

IGCN – 5th Floor. Department: 493006

Manager:

Patrick Evans

What We Do:

Manage Active Directory (AD) domain services for the organization, which is the backbone for authentication and name resolution (DNS). The AD team is responsible for design, implementation, security hardening, disaster planning, recovery, management and troubleshooting of Active Directory infrastructure issues. In addition to Active Directory, we also maintain Azure Active Directory for use with Azure AD integrated applications including Office 365 as well as ADFS, MFA, Azure AD B2B and B2C services.

Our Products:

Microsoft Active Directory, Microsoft Active Directory Federation Services, Microsoft Azure Active Directory, Microsoft Azure Active Directory B2B, Microsoft Azure Active Directory B2C, Microsoft AD Connect, Microsoft MFA Server, Microsoft Identity Management Server

Our Tools:

ASM Ticket Management and SLA Measurement

Our Metrics:

Resolve customer issues within 2 IOT business days 90%+ G; 87%+ Y; <87% R

Mon-Fri 6am-6pm excluding state holidays

Our customers:

39,000+ state employees and contractors, 5000+ Service and resource accounts, 6000 Guest business partner accounts and 500000 constituent B2C accounts.

Our Budget:

Please see Seat

Major Accomplishments:

- Completed migration of end users/applications/infrastructure from current on-premises MFA environment (Azure MFA Server) to one hosted in the cloud (Azure AD MFA) in order to modernize the state's MFA and provide for a more secure environment.
- Completed the replacement of our Azure AD Connect infrastructure. This was done to remediate issues faced within our AD Connect environment and to provide for more flexibility as our footprint continues to expand.
- Added two new team members to the group via the IOT State Earn and Learn (SEAL) program, in order to give the participants the opportunity to learn the technology and processes associated with the IAM team.

Current Projects:

- Active Directory domain controller (DC) upgrade project which will include the separation of DNS from our DCs and an upgrade of windows server operating systems currently on those devices from 2012 to the most current version available.
- After completing an assessment of our Active Directory, and to better manage our infrastructure and reduce the exposure of our environment to cyberattacks, we are working, with the help other IOT stakeholders, to sanitize our Active Directory environment. This includes the cleanup and removal of stale/disabled accounts, GPOs, OUs, and user objects.
- The IAM team has begun communicating with legacy application owners in order to decommission or migrate apps/resources away from ADFS and into Azure AD. Our plan is to move as many resources off ADFS as possible by the end of Q1 2023.