Process

Title:	ODHSOHA 090-003-13 Service Account Request and Password Process
Related to:	ODHSOHA 090-003 Access Control
Effective date:	12/04/2023

Purpose

A service account is used to execute applications and run automated services and other processes. The security context determines the service account's ability to interact with local, network, and cloud resources. The purpose of this process is to outline the steps to obtain a service account for information technology (IT) system tasks for ODHS and OHA.

Applicability

This process applies to all ODHS and OHA staff including employees, volunteers, trainees, interns, as well as contractors and partners. This process applies to Active Directory and cloud hosted identity providers only.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Process Steps

1. The use of standalone Managed Service Accounts (sMSAs) and group Managed Service Accounts (gMSAs) are recommended for ODHS and OHA staff because passwords are automatically generated.
   a. sMSAs are a type of domain account created and managed by the domain controller for use running a service.
   b. gMSAs provide the same functionalities as sMSAs and extend that functionality over multiple servers.
2. Service account requestors, including ODHS and OHA staff, partners, and contractors, obtain approval from an ODHSOHA manager and the information system owner or designee for service account creation.

3. The requestor submits an Office of Information Services (OIS) Service Desk ticket for service account creation with the approvals obtained in process step two.
    a. When technically feasible, accounts will be restricted to systems identified in the request.
    b. Requests should include if the password is standard, non-expiring, or enabled for cloud sign in.
4. If a service account is requested for use by non-ODHS and OHA staff, the requestor provides the associated Access Agreement number in the Service Desk ticket.
    a. OIS Identity and Access Management team verifies the Access Agreement number in the Service Desk ticket.
    b. If there is not an associated Access Agreement number, OIS ID and Access Management team refers the requestor to the Information Exchange Coordinator at dhsoha.infoex@odhsoha.oregon.gov.
5. OIS ID and Access Management team validates the request and assigns to the OIS infrastructure operations team for creation.
6. The OIS infrastructure operations team sets up the requested service accounts and communicates the temporary credentials to the requestor.
7. The OIS infrastructure operations team closes the Service Desk ticket when the request has been fulfilled.
8. The requestor changes the temporary password upon initial login, within seven business days.
9. Owners of service accounts accessing ODHS and OHA information systems follow these requirements for service account password assignment:
    a. Create passwords that meet complexity standards.
    b. Change service account passwords every 180 days.
    c. Restrict to specific devices and hours when possible.
    d. Assign permissions based on the principle of least privilege.
    e. Prohibit sharing service account credentials.
10. Passwords are composed of the following:
    a. At least sixteen (16) characters long.
    b. At least one character from each of these categories:
        A. Uppercase letter (A-Z)
        B. Lowercase letter (a-z)
        C. Numeral (0-9)
        D. Special character (% @ # $! * / + > < [ ] { } \ -)
    c. ePasswords will not be set to one of the last 24 previously used passwords.

11. Exception requests for non-expiring passwords require a 64-character minimum password length and meet active directory complexity requirements. Regulatory compliance is the sole responsibility of the service account owner.
12. If a service account connects to cloud services, it must have a 64-character minimum password and meet active directory complexity requirements.
13. ODHS and OHA information systems and applications will not display passwords in plain text when entered and will not transmit unencrypted passwords.

References

Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite Volume I: Harmonized Security and Privacy Framework Version 2.2

National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations

National Institute of Standards and Technology Internal Report (NISTIR) 7966 Security of Interactive and Automated Access Management Using Secure Shell (SSH)

Microsoft Learn/Windows Server/Service Accounts

Statewide Information and Cyber Security Standards

ODHSOHA 090-003-04 Managing Password Process

ODHSOHA 090-003-05 User Access Process

ODHSOHA 090-003-08 Third Party Entity Approval for System Access Process-Partners

ODHSOHA 090-003-010 Third Party Entity Approval for System Access Process-Contractors

ODHSOHA 090-003-014 Service Account Request and Password Process Map

Related policies

DAS 107-004-052 Cyber and Information Security

DAS 107-004-110 Acceptable Use of State Information Assets

ODHSOHA 090-003 Access Control Policy

Contact

Office of Information Services
Service Desk: 503-945-5623
OIS.ServiceDesk@odhsoha.oregon.gov

Process History

Version 1 DHS|OHA 090-003-013 established 11/05/2018

Version 2 ODHS|OHA 090-003-013 revised 05/03/2021

Version 3 ODHSOHA 090-003-13 revised with additional password process added from ODHSOHA 090-003-15 12/04/2023

Keywords

Access, account, group Managed Service Accounts, gMSAs, Managed Service Accounts, sMSAs, password, requestor, service, service account, temporary credentials

---

This document can be provided upon request in an alternate format for individuals with disabilities or in a language other than English for people with limited English skills. To request this document in another format or language, contact the Publications and Design Section at 503-378-3486, 7-1-1 for TTY, or email dhs-oha.publicationrequest@state.or.us.