Access Control Security Specifications

Last revised: December 2018
Last reviewed: December 2018
Next review: December 2019

Information Security Branch, Ministry of Central Services

This document outlines the Government of Saskatchewan security specifications for Access Control.

Table of Contents

Reference Documents

The following documentation is available on the IT Security Services Taskroom:

- *Access Control Security Policy*
- *Access Control Security Standard*

Government of Saskatchewan

1. Access Control Standard for Windows Service Accounts

Windows service accounts are required for various services to function on Windows servers providing services to Ministries. As the stability of these accounts impacts the availability of services they may fall outside of the standard account definition. This standard describes the requirements for all Windows service accounts. Accounts that meet the defined service account requirements do not require a Risk Management Decision Item (RMDI) as the risks are known and understood to be the same for all Windows services accounts. The requirements listed below provide a mechanism to ensure that risks associated with deviating from the standard user account and password policies/standards are reduced.

Windows Service Accounts within the Government of Saskatchewan computing environment must meet all of the following requirements:

- the account does not allow interactive logins; end users will not be able to enter the account username and password to access network and domain resources on the government network;
- the account will be used for a specific function;
- the account has a defined account owner who is authorized to request changes related to the service account and is responsible for ensuring the security of the account password;
- the account password is randomly generated and has a minimum of 30-50 characters and includes upper and lower-case letters, numbers and special characters, does not repeat three characters or more in a row, and does not include any dictionary words;
- the account password is provided only to the appropriate people at the time of service registration or adding batch processing jobs to the scheduling service and cannot be shared with any unauthorized individuals;
- the password will not expire but must be changed manually every 365 days; this can be done as part of a regular maintenance cycle; reports will identify any service account password that has exceeded the 365-day maximum age and remediation will be required immediately.

2. Access Control Standard for UNIX Service Accounts

This specification describes the requirements and attributes which will be used to classify a UNIX service account.

UNIX service accounts are required to run services on various UNIX servers. The maintenance and operation of UNIX services often requires execution of commands under the service account. UNIX systems allow for this through the use of sudo which eliminates the need for users to directly log into the system with service account credentials by allowing them to run specific commands with the privileges of the service account from their regular user account.

UNIX service accounts which adhere to the attributes and requirements listed below are considered to be compliant with security standards and do not require an RMDI.

The following requirements and attributes are used to define a compliant UNIX service account within the Government of Saskatchewan:

- service daemons must run under a service-specific account and must not be the root user nor have a user identifier (UID) of 0 (zero);

  There may be instances where a service control command must be executed as the root user, however, the daemon process should not be running as the root user. Access to the root user account via sudo should be restricted to system administrators only and any commands requiring execution as the root user should be executed by system administrators with the appropriate access.

- the service account must not allow interactive logins; this can be achieved by ensuring that the default shell for the account is a null shell appropriate for the platform, typically /bin/false;
- the encrypted password for the service account must be null or an invalid entry to prevent direct login to the account;
- the service account must not have sudo access to other accounts;
- the service account will be set to "password does not expire;" there is no password to change so there is no need for manual password changes;
- an owner for the service account must be defined; the account owner will have the authority to request changes to the account.

3. sudo Configuration Requirements

Users may be granted access to service accounts through the sudo facility on UNIX systems. The use of sudo to access service accounts ensures that proper audit logging is maintained at all times. A restricted list of commands with the full path will be provided for inclusion in the sudo configuration as the command set for a specific service account. Command sets will be requested by the various functional groups within Information Technology Division and with service providers. Information Security Branch will review requested command sets to ensure that the command set does not include binaries which could be used to execute a shell as the service account as executing a shell would circumvent audit logging.

The ability to access service accounts via sudo may be achieved either by identifying specific users or groups in the config file. If groups are granted sudo access to a service account, the group must not be a default system group. Groups should be created with role-specific access in mind.

4. Other Access Considerations

Other means of accessing non-user accounts on UNIX systems may currently be in place. For example, the use of authorized keys for SSH can allow users to access an account remotely through the secure shell or secure FTP. Authorized keys should be configured with a passphrase that meets the current password complexity specification. The use of blank passphrases for authorized keys is prohibited. Exceptions require acceptance of risk via the Risk Management Decision Item process.

5. Group Managed Service Accounts and Managed Service Accounts

Group Managed Service Accounts (GMSAs) are managed domain accounts that provide automatic password management and simplified Service Principal Name (SPN) management. This includes delegation of management to other administrators on individual servers or over multiple servers (i.e. clusters, server farms). When GMSAs are used as service principals, the Windows operating system manages the password for the account instead of relying on the administrator to manage the password.

GMSAs must be used on a go forward basis for new applications and upgrades.

GMSAs are compatible based on the application/function that is using the service account. They will have to be evaluated on a case-by-case basis.

Existing services accounts won't be reviewed unless the application undergoes an upgrade and the opportunity exists to review the service account.

On servers running Windows Server 2012 and newer, GMSAs must be used where the following conditions are true:

- the service account does not require interactive logins to be enabled;
- elevated privileges are not required by the service account;
- the application requiring a service account is certified to support GMSAs.

6. Managed Service Accounts

On servers running Windows Server 2008 R2 up to Windows Server 2012 managed services accounts (MSAs) must be used where the following conditions are true:

- GMSAs are not supported by the application;
- the service account does not require interactive logins;
- elevated privileges are not required by the service account;
- the application is capable of supporting service accounts using Kerberos encryption types.

7. Specifications for Authentication Credentials

The purpose of this specification is to prevent unauthorized access to sensitive information. The data classification as determined by a Statement of Sensitivity and the policies and standards for Asset Management is used to determine the appropriate authentication controls to apply.

7.1. Public – Low

This level applies to read-only public data that uses authentication for purposes other than access control, such as to retain user personalization or configuration. This level requires authentication of a single-factor credential with low security requirements.

An electronic credential for the handling of non-sensitive information must use either:

a. a simple password (not required to comply with the *Password Standards* section of the Access Control standards); or
b. an assertion from another authentication service that uses any credential strength and authentication method and that is deemed by the relying party to be an authoritative and trusted service.

7.2. Class C – Medium

This level applies to sensitive information with low injury in the event of a disclosure. This level requires authentication with a single-factor credential.

An electronic credential intended to achieve a medium credential strength must use either:

a. a password that conforms to the Password Standards section of the Access Control standards;
b. an assertion from another authentication service that uses a comparable or higher credential strength and authentication method (Class C to A); or
c. a software- or hardware-based multifactor authentication system approved by Information Technology Division; it may or may not conform to the higher credential strength (Class B or A) standards (e.g. a one-time password device that is not FIPS 140-2 compliant).

7.3. Class B – High

Class B data accessed external of the electronic security perimeter requires encryption; internal to the GOS network encryption is not required.

An electronic credential intended to achieve a high credential strength must use either:

a. a cryptographic token that:
    i. uses a key and cryptographic mechanism compliant with FIPS 140-2 Level 1 or higher and that is approved by the Information Technology Division;
    ii. requires either 1) the use of a password or biometric by the individual to activate the cryptographic mechanism or 2) a password in combination with the cryptographic mechanism in the same authentication protocol; and
    iii. follows the Password Standards section of the Access Control standards;
b. a one-time password device token that:
    i. depends on a symmetric key stored on a personal hardware device that is a cryptographic module compliant with FIPS 140-2 Level 1 or higher;
    ii. permits at least 106 possible password characters; and
    iii. requires the use of a password or biometric by the individual to activate the retrieval or generation of the one-time password;
c. an assertion from another authentication service that uses a Class B or Class A credential strength and authentication method (Class B or A).

7.4. Class A – Very High

This level applies to highly sensitive information. It requires multifactor authentication with a cryptographic token.

An electronic credential intended to achieve a very high credential strength must use a hardware-based cryptographic token that:

a. uses a key and cryptographic mechanism stored on a special hardware device validated at FIPS 140-2 Level 1 at a minimum;

b. requires either 1) the use of a password or biometric by the individual to activate the cryptographic mechanism or 2) a password in combination with the cryptographic mechanism in the same authentication protocol; and

c. follows the Password Standards section of the Access Control Standards for any password used.