Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guideline on Cloud Authentication

Published: 2024-12-02

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-51/2024E-PDF
ISBN: 978-0-660-74624-1

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Ligne directrice sur l’authentification en nuage

Guideline on Cloud Authentication

From: Treasury Board of Canada Secretariat

On this page

1. Introduction

▶ In this section

1.1 Background

Authentication is the process of verifying the identity of a user, process or device, often before allowing access to resources in an information system. [1] In the context of cloud, and as outlined in the *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)*, organizations are responsible for ensuring that individuals and devices are uniquely identified and authenticated before being granted access to information and information systems hosted in a cloud service provider (CSP) environment. Effective authentication is essential to keeping accounts secure.

1.2 Purpose and Scope

This document provides advice and recommendations on how internal users, namely privileged and non-privileged Government of Canada (GC) users (such as employees and contractors) should be authenticated when accessing GC services hosted in the cloud. This document does not address authentication of external users accessing online GC services hosted in the cloud (or otherwise).

This document replaces the *Guidance on Cloud Authentication for the Government of Canada* document, dated August 23, 2018. Over time, recommendations made in this document may be updated and/or subsumed by other policy instruments, and this document will be updated accordingly.

1.3 Applicability

This document applies to GC organizations that are adopting cloud services. Specific applicability statements are made where appropriate (for example, where recommendations may differ depending on the organization's service delivery model).

1.4 Audience

This guide is for Information Technology (IT) practitioners and IT security practitioners who are acting in any of the following roles:

- project manager
- business analyst
- requirements analyst
- enterprise, security and solution architect
- system and software designer
- security design specialist
- system and system security engineer
- system, software, and security integrators and testers

- security assessors

1.5 Requirements

The following are authentication requirements from various Treasury Board policy instruments:

1.5.1 Deputy heads are responsible for identifying security and identity management requirements for all departmental programs and services, considering potential impacts on internal and external stakeholders (section 4.1.4).
Reference: Policy on Government Security [1]

1.5.2 Implement measures to ensure that individuals and devices are uniquely identified and authenticated to an appropriate level of assurance before being granted access to information in information systems, in accordance with Appendix A: Standard on Identity and Credential Assurance of the Directive on Identity Management (section B.2.3.1)
Reference: Appendix B: Mandatory Procedures for Information Technology Security Control of Directive on Security Management [2]

1.5.3 Program and service delivery managers are responsible for using mandatory enterprise services for identity management, credential management and cyber authentication (section 4.1.9).
Reference: Directive on Identity Management [3]

1.5.4 Organizations must identify and authenticate individuals and devices to an appropriate level of assurance before being granted access to information and services hosted in cloud services. Such authentication is in accordance with the Standard on Identity and Credential Assurance and aligns with GC enterprise identity and authentication services (section 6.2.3).
Reference: Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN 2017-01) [4]

1.5.5 Deputy heads are responsible for using enterprise or shared IT solutions, assets and services to avoid duplication, when available and appropriate (section 4.4.2.3).
Reference: Policy on Service and Digital [5]

1.5.6 Authentication hardening:

1.5.6.1 Authenticate users before they are granted access to a system and its resources, leveraging approved Government of Canada authentication services, in accordance with the *Directive on Identity Management* and associated guidelines. Exceptions are to be assessed through the GC Enterprise Architecture Review Board.

1.5.6.2 Implement strong authentication mechanisms such as multi-factor authentication (MFA) for all accounts that have privileged or enhanced access, in accordance with Canadian Centre for Cyber Security guidance in ITPS.30.031 v3, User Authentication Guidance for Information Technology Systems. Additional information regarding the GC enterprise approach with respect to MFA is provided in Multi-factor Authentication Considerations and Strategy for GC Enterprise IT Services. At a minimum, MFA is used to authenticate:

1.5.6.2.1 All users accessing information systems with an Assurance Level Requirement of 3 or higher;

1.5.6.2.2 All privileged users performing privileged actions; and

1.5.6.2.3 All users of remote access solutions.

1.5.6.3 Where passwords are used, implement a password policy in accordance with the GC *Password Guidance*.

1.5.6.4 Systems are configured with a session or screen lock.

1.5.6.5 Systems have an approved log-on banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Reference: Account Management Configuration Requirements of Appendix G: Standard on Enterprise Information Technology Service Common Configurations [6] of the Directive on Service and Digital [7]

1.5.7 Protect user accounts and identities. (Guardrail #1).

Manage access (Guardrail #2).

Reference: Version 2.0 of the GC Cloud Guardrails [8] of Appendix G: Standard on Enterprise Information Technology Service Common Configurations [6] of the Directive on Service and Digital [7]

2. Implementation Guidance

▶ In this section

To adhere to the policy requirements identified in section 1, section 2 outlines implementation guidance for GC organizations.

For additional enquiries and interpretation of this section, contact TBS Cyber Security Division.

2.1 Enforce multi-factor authentication for all users

To keep credentials secure and prevent unauthorized access to cloud-based services, user access is expected to be protected with strong multi-factor authentication (MFA), in accordance with the Account Management Configuration Requirements [6] and related guidance documents. Wherever and whenever possible, phishing-resistant MFA options should be used.

2.2 Adopt appropriate authentication solutions

The section outlines considerations for authentication solutions depending on the following operating context, including:

- hybrid environments with a combination of on-premises and cloud-based resources

- environments with cloud-only resources

The GC is exploring additional identity modernization approaches and the related models for using a hybrid identity architecture. Guidance will be updated as this work proceeds.

2.2.1 For environments with on-premises and cloud resources

Organizations that have resources on premises and in the cloud (hybrid deployment model for departmental data and applications) are expected to use federated authentication for non-privileged users. [2]

In this configuration, the user authentication process can continue to take place on-premises, allowing the user to log on once to access both on-premises and cloud-based resources. This supports single (or simplified) sign on and reduces credential sprawl and password reuse. [3]

The use of federated authentication has the following benefits:

- authentication policies are not transmitted externally
- the risk of potential exposure of on-premises passwords in the cloud during the user authentication process is minimized in particular for organizations that have on-premises data and services that are deemed too sensitive to migrate to the cloud (see Appendix A-2 for more information)
- all authentication transactions are handled in one place, ensuring that each account only needs one record, facilitating central policy management and logging for all authentication attempts
- federation is based on open, industry accepted standards and is therefore independent from any CSP specific (or proprietary) authentication solutions
- there is no dependency on one CSP to broker access to other CSPs

Organizations are expected to use enterprise or shared IT solutions, assets and services to avoid duplication, when available and appropriate. To that end, organizations can use enterprise services that support federated

authentication with CSPs that are available from Shared Services Canada (SSC). This includes the Active Directory Federation Service (AD FS) and GCpass, which provide a secure and scalable federated authentication capability that allow users to authenticate to cloud-based services using their GC credentials.

For organizations not within scope of SSC services and having limited IT resources, an options analysis and risk assessment should be performed to determine the most suitable user authentication option based on their business, technical and threat context.

Refer to Appendix A for additional security considerations for the protection of federation services.

2.2.2 For environments with cloud only resources

While there are many benefits to handling all authentication centrally, organizations that have moved all their departmental data and applications to the cloud may want to take advantage of cloud-based identity services for user authentication rather than continue to operate their own infrastructure components, particularly for departments that have limited IT resources.

Organizations should conduct an options analysis and risk assessment to determine the most suitable user authentication method based on their business, technical and threat context. The assessment should include security considerations, user experience, [4] infrastructure requirements, operational burden and cost, reliability and disaster recovery implications, among other things.

While not meant to be exhaustive, the following are considerations that will have an impact on the selection of the most suitable cloud authentication method and should be included in the aforementioned analysis:

- an organization that operates its own credential management infrastructure may benefit from managing credentials using a CSP

provided platform, as this eliminates the need for the organization to maintain and operate separate infrastructure

- an organization that uses more than one CSP will need to consider that each user may need multiple credentials if the organization is not using federation services. To prevent credential sprawl, organizations should minimize the number of credentials needed to access cloud-based services. Conversely, if an organization uses one CSP to broker access to another CSP, the organization will need to consider increased dependency and resiliency to account for failures in the CSP providing brokering services
- the self-service password recovery features supported by the CSP may not be adequate and may need to be improved before it can be used (see section 2.4 for additional information); therefore, the organization may need to manage password recovery
- incompatibility of cloud primary authentication with legacy applications may necessitate a departmental instance of Active Directory (AD) either on-premises or in the cloud, even though all other data and applications are hosted in the cloud

Refer to Appendix A for additional security considerations for password synchronization authentication.

2.3 Ensure adequate protection of cloud administrator accounts

As with on-premises privileged accounts, protecting against unauthorized access to cloud privileged accounts is essential and is subject to the following configurations:

2.3.1 Support privileged access to cloud services through appropriate security controls, in accordance with the Communications Security Establishment's (CSE's) *User Authentication Guidance for Information Technology System (ITSP.30.031v3)* [9]

2.3.2 restrict access to personnel based on the principles of least privilege, need to know, and segregation of duties

2.3.3 protect access to all privileged accounts (whether in the cloud or on-premises) using strong MFA solutions, and phishing-resistant MFA is strongly recommended [5]

2.3.4 use different credentials to access privileged accounts in the cloud from those used for administrating on-premises resources

2.3.5 to reduce the blast radius of credential attacks between on-premise and cloud environments, ensure that highly privileged cloud administrative users, groups and roles (such as global administrator/root) are not included within scope for synchronization from on-premises environments, and are not used with federated SSO, but instead rely on cloud-native authentication; [6] however, this is not meant to preclude the use of federation for less privileged administrators such as application/SaaS administrators, particularly when the benefits of federation outweigh cloud-native authentication

2.3.6 disable cloud based self-service password reset (SSPR) capabilities for cloud administrators

2.3.7 where available, configure admins to be “eligible” for a role and request activation for the least privilege role required, only when the role is needed and only for a limited period of time

2.3.8 do not allow self-approval of activation requests for highly privileged cloud administrative roles (for example, root, Global admin) [7]

2.3.9 where available, enforce attribute-based access control (ABAC) to restrict access based on a combination of authentication factors (such as MFA), managed devices, device compliance, sign-in and user risks, and location

2.3.10 audit, review and monitor all privileged access and actions in accordance with the sensitivity of the access

2.3.11 implement applicable requirements as specified in Appendix G: Standard on Enterprise Information Technology Service Common Configurations of the Directive on Services and Digital [7]

2.4 Understand the implications of using cloud-based self-service password reset

SSPR method(s) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work.

This ability reduces help desk calls and loss of productivity when a user cannot sign into their device or an application. However, the SSPR must be at least as secure and robust as the method(s) used to obtain the primary authenticator to be recovered.

Based on section 2.3, it is recommended that cloud-based SSPR capabilities be disabled for all cloud administrators. This also applies to all privileged accounts, whether on-premises or in the cloud. Furthermore, cloud-based SSPR is not recommended for resetting on-premises passwords even for non-privileged users, since this exposes the GC to a higher level of risk, which can be avoided through federation.

Alternatives to cloud-based SSPR include one or more of the following:

2.4.1 continue to use existing internal password reset methods

2.4.2 reset passwords using video conferencing with help desk personnel to demonstrate the user is who they claim to be (for example, using a valid GC-issued picture ID, such as a building pass, over MS Teams or other video chat capability, preferably using a GC-managed device if possible)

2.4.3 follow GC Password Guidance [10], which includes recommendations that will make passwords easier to remember and

eliminate password expiration (passwords should only be changed when compromise is suspected or known)

For additional information related to Azure AD SSPR, refer to the discussion paper for Considerations for Using Microsoft Azure AD SSPR within the GC (available upon request by contacting the TBS Cyber Security Division).

2.5 Monitor authentication events for security threats

Security monitoring, alerts and machine learning–based reports that identify inconsistent access patterns will help to identify possible security risks. An active identity monitoring system can quickly detect suspicious behaviour and trigger an alert for further investigation. This includes monitoring events such as:

2.5.1 anomalous access patterns

2.5.2 brute force attacks against a particular account

2.5.3 attempts to sign in from multiple locations

2.5.4 sign-ins from infected devices

2.5.5 suspicious IP addresses

2.5.6 use of weak/legacy authentication protocols

2.5.7 lateral movement patterns

2.5.8 privilege escalation

2.5.9 persistence techniques

Without knowing that suspicious activities are taking place through these credentials, it will be hard to mitigate this type of threat. The GC Event Logging Guidance [11] provides additional guidance on events to configure to support security operations and monitoring.

3. References

1. Treasury Board of Canada Secretariat, “Policy on Government Security”
2. Treasury Board of Canada Secretariat, “Directive on Departmental Security Management”
3. Treasury Board of Canada Secretariat, “Directive on Identity Management”
4. Treasury Board of Canada Secretariat, “Direction on the Secure Use of Commercial Cloud Services,” November 2017
5. Treasury Board of Canada Secretariat, “Policy on Service and Digital”
6. Treasury Board of Canada Secretariat, “Appendix G: Standard on Enterprise IT Service Common Configurations - Account Management Configuration Requirements”
7. Treasury Board of Canada Secretariat, “Directive on Service and Digital”
8. Treasury Board of Canada Secretariat, “GC Cloud Guardrails”
9. Canadian Centre for Cyber Security, “User authentication guidance for information technology systems (ITSP.30.031 v3)”
10. Treasury Board of Canada Secretariat, “Password Guidance”
11. Treasury Board of Canada Secretariat, “Event Logging Guidance”
12. Microsoft, “Implement password hash synchronization with Azure AD Connect sync”
13. Canadian Centre for Cyber Security, “Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111”
14. Microsoft, “Password hash synchronization and FIPS”
15. National Security Agency, “Detecting Federated Authentication Abuse”
16. Treasury Board of Canada Secretariat, “GC ICAM Reference Framework”
17. National Institute of Standards and Technology, “Digital Identity Guidelines (SP800-63-3)”

Appendix A – Additional Security Considerations

▶ In this section

A-1 Federation Services

Federation with any environment depends on trust in the components that perform user authentication and digitally sign the federation protocol (SAML or OpenID Connect) messages. If these components are compromised, they can be exploited to obtain unauthorized access to resources. Therefore, it is critical that all federation components and services are properly configured for secure operation. At a minimum, this includes:

A-1.1 configure all federation components and services in accordance with available guidance (vendor supplied or otherwise [8])

A-1.2 continuously monitor for anomalous activity both on-premises and in the cloud

A-1.3 store private keys used to digitally sign SAML and OpenID Connect assertions/claims in a FIPS 140-2 or FIPS 140-3 Level 2 overall (with Level 3 physical security) or higher validated hardware security module (HSM) [9]

A-1.4 treat all federation components as critical assets and adhere to secure privilege access best practices

Exploitation of on-premises identity services could lead to unauthorized access of cloud environments. Therefore, it is recommended that highly privileged accounts in the cloud identity service and SaaS public cloud applications be excluded from federation and remain as “cloud-only” accounts to limit lateral movement from a compromised on-premises environment to the cloud, therefore reducing the blast radius.

Based on section 2.2.1 of this document, organizations are encouraged to use existing GC enterprise federation services. However, in exceptional circumstances, an organization may choose to deploy a bespoke federation solution to satisfy specific business or departmental requirements that may not be available with enterprise solutions. In this scenario, organizations should ensure that the authentication solution:

A-1.5 provides a positive user experience

A-1.6 adheres to applicable security requirements, including those identified in this section

A-1.7 adheres to industry best practices

A-1.8 uses existing capabilities for authentication wherever possible to minimize the proliferation of bespoke solutions

A-1.9 follows all relevant GC policies and guidance, including the requirements specified in this guidance document

Organizations must contact Treasury Board of Canada Secretariat (TBS) Cyber Security Division before using a bespoke cloud authentication solution.

A-2 Password Synchronization Authentication

Password synchronization authentication, such as Microsoft's Password Hash Synchronization (PHS) feature supported by Microsoft Azure Active Directory (AD) [12], is another configuration option for authentication.

For organizations that fall under the category of section 2.2.2 of this document, the following outlines additional considerations when using password synchronization authentication, including:

A-2.1 when syncing passwords, the use of hashing mechanisms and encryption is paramount to preserving the confidentiality and integrity of account credentials, in alignment with the Canadian Centre for Cyber

Security's guidance Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information (ITSP.40.111) [13]

A-2.2 ensure that MFA is enforced for all users prior to enabling password synchronization

A-2.3 exclude the synchronization of any accounts that are not required to be used in the cloud, including service accounts used on-premises or IaaS-based servers, or highly sensitive administrative accounts used to administer on-premises or IaaS-based servers (such as domain admins, global admins, root, and any domain admin equivalent access)

A-2.4 ensure SSPR and password writeback are disabled (see guidance in section 2.4 of this document)

A-2.5 take steps to synchronize expired on-premises AD accounts with Azure AD. The account Expires attribute of Windows AD accounts is not synchronized to Azure AD. As a result, an expired on-premises AD account configured for password synchronization authentication (PHS) will still be active in Azure AD. If the account expiration feature is used, it is recommended that organizations implement a service desk workflow or an automated process to also disable the user's Azure AD account (use the Set-AzureADUser cmdlet)

A-2.6 use the default "never expire" password setting; this is consistent with GC Password Guidance [10] and should not be overridden

A-2.7 ensure that MD5 is enabled in accordance with applicable Microsoft documentation [14] [10]

In addition, organizations that use AD FS to federate with Microsoft Azure AD may be aware that PHS can be enabled to support certain security features such as credential leakage detection. This guidance does not preclude the use of PHS for this purpose. In other words, it is possible to implement federated authentication via AD FS and enable PHS to support credential leakage detection (but not for user authentication).

Furthermore, for resiliency purposes, organizations that are operating their own AD FS infrastructure may be contemplating the use of PHS as a backup for their primary authentication method (federation). However, as discussed in section 2.2.1 of this document, the benefit of using federated authentication for hybrid environments is to minimize the risk of exposing on-premises credentials in the cloud during the user authentication process.

Organizations should perform an options analysis and risk assessment that consider the trade-offs between security and availability based on the organization's business, technical and threat context. If an organization does elect to use PHS as a backup, any users who have logged on directly to Azure AD should be required to reset their passwords once the AD FS infrastructure components have been restored.

---

1 According to the Government of Canada Identity, Credential, and Access Management (GC ICAM) Reference Framework [16] and the NIST SP800-63-3 Digital Identity Guidelines [17]

2 See section 2.3 for additional guidance with respect to privileged users.

3 Major CSPs such as Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure support federation via Active Directory Federation Service, so the same infrastructure can be used to support user authentication to multiple CSPs.

4 For example, minimize the number of credentials needed to access cloud-based services.

5 Credentials used to access emergency access accounts (sometimes referred to as “break glass” accounts) may be based solely on a very strong, strictly controlled user ID/password. Use of two-person control to help prevent unauthorized access to these special accounts is strongly recommended.

6 See the NSA bulletin Detecting Abuse of Authentication Mechanisms [15] for further information and rationale.

7 For example, manager approval may be required for highly privileged roles.

8 Specific guidance related to federation with Azure AD is provided in the NSA bulletin Detecting Abuse of Authentication Mechanisms [15].

9 See the NSA bulletin Detecting Abuse of Authentication Mechanisms [15] for further information and rationale.

10 This is not meant as an endorsement of MD5 or meant to conflict with GC guidance on cryptography. It is simply a function of Microsoft’s implementation.

Date modified:

2024-12-02