# Cloud Console Access

## Objective

Limit access to GC managed devices and authorized users.

## Key Considerations

* [ ] Implement multi-factor authentication mechanism for privileged accounts and remote network (cloud) access.
* [ ] Determine access restrictions and configuration requirements for GC managed devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly.

**Note:** Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access.

* [ ] Ensure that administrative actions are performed by authorized users using a trusted device that is connected to a trusted network (e.g. GC network).
* [ ] Implement a mechanism for enforcing access authorizations.
* [ ] Implement password protection mechanisms to protect against password brute force attacks.

## Validation

* [ ] Confirm policy for MFA is enabled through screenshots and compliance reports.

## Additional Considerations

* [ ] Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attributed-based access control (ABAC).

## Applicable Service Models

* IaaS, PaaS, SaaS

## References

1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3
2. CSE Top 10 #2
3. Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp)
4. Related security controls: AC‑2, AC‑2(1), AC‑3, AC‑5, AC‑6, AC‑6(5), AC‑6(10), AC‑7, AC‑9, AC‑19, AC‑20(3), IA‑2, IA‑2(1), IA‑2(2), IA‑2(11), IA‑4, IA‑5, IA‑5(1), IA‑5(6), IA‑5(7), IA‑5(13), IA‑6, IA‑8