Why shared logins and unique user IDs matter for CPCSC MFA requirements

When a Canadian defence supplier prepares for CPCSC Level 1 compliance, one of the more subtle areas is the evidence required around multi-factor authentication (MFA). The ITSP.10.171 control asks for more than just turning MFA on. It expects the supplier to show that MFA is applied to every interactive user account, and that those accounts are individually identifiable. That second part - unique user IDs - is where many organisations run into trouble, especially when external partners or suppliers share logins to a system.

What the control actually asks for

The ITSP.10.171 requirement, in plain language, says that MFA must be used for all administrative access and for any access to the protected system from outside its boundary. But the underlying principle is that each person who accesses the system has their own account. Shared logins, where two or more people use the same user ID and password, effectively break MFA. Even if a shared login has MFA enrolled, the second factor is tied to the account, not to the individual. You lose the ability to know who actually authenticated.

This matters for audit and incident response. If a breach happens and the log shows only a generic account name, you cannot tell which person was responsible. The control is designed to prevent exactly that gap.

Shared login risks in supplier environments

Supplier environments are a common place where shared logins appear. A third-party technician needs temporary access to a system to run a diagnostic or apply a patch. Instead of creating a dedicated account for that person, an organisation hands over a generic admin login that everyone on the vendor team uses. The rationale is speed: the technician needs access now, and provisioning a new account takes time. But the risk is real.

When multiple people share a single account, MFA becomes a shared secret too. The token or one-time code is passed around, copied, or stored in a shared document. That defeats the purpose of the second factor. An attacker who obtains the shared password and the shared token can move through the system as a legitimate user, and nobody can trace which session belonged to the attacker versus the vendor.

Another scenario is a long-term contractor who is given a group permission set rather than a personal account. The contractor's access is tied to a role, not to their identity. When the

contractor leaves, the role remains, and someone else inherits the permissions without a formal review. This is where account inventory and regular access reviews become essential.

How MFA enrollment works with unique IDs

MFA enrollment is straightforward when every user has a unique account. The administrator registers a second factor - a mobile authenticator app, a hardware token, or a biometric - for that specific person. The system then knows that when that token is used, it was the account owner who authenticated.

With a shared login, you cannot enroll MFA per person. The token is shared, or worse, the MFA is disabled entirely because it is impractical to hand a hardware token around a team. The result is a gap in the compliance evidence. An auditor reviewing the supplier's MFA configuration will look for proof that every interactive account has MFA enforced. A shared account without MFA, or with MFA shared among many users, will flag as non-compliant.

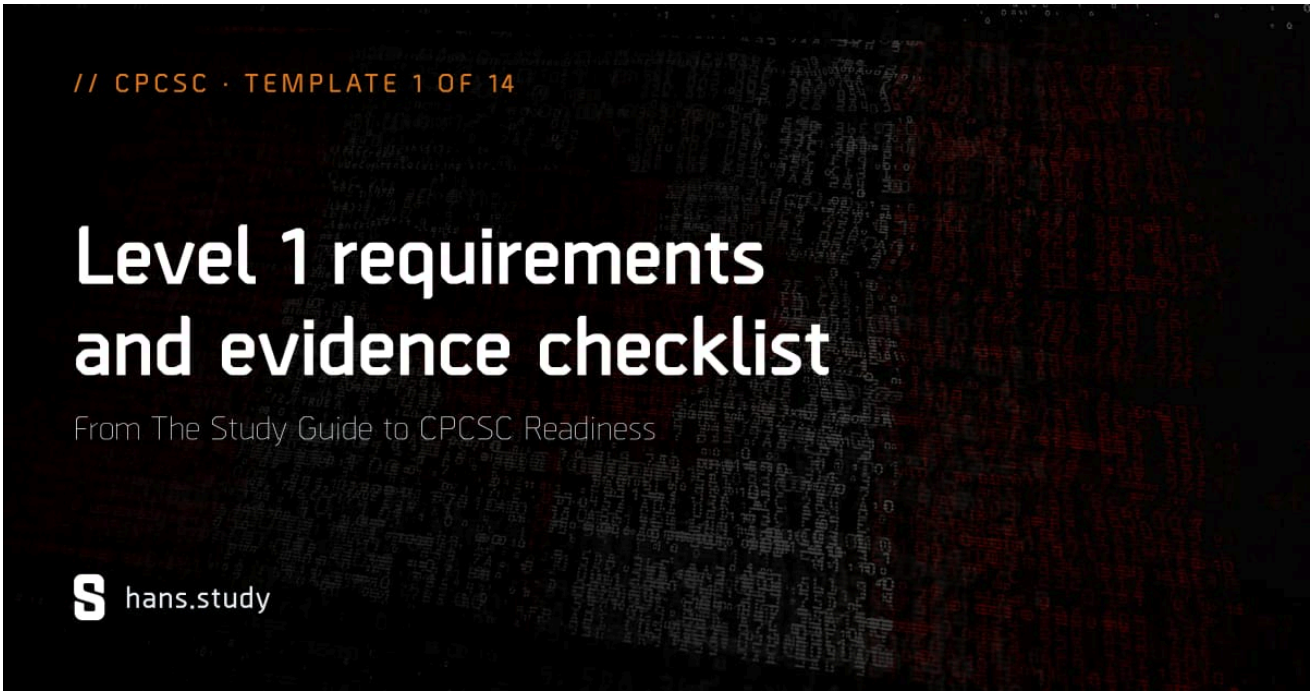
Device identification and group permissions

Some systems support device identification as an additional factor. A recognised device can act as a second factor if the user logs in from a known machine. This works well when each person has a dedicated workstation. In a supplier environment, where technicians use different laptops on different days, device identification becomes unreliable. The system might not recognise the device, forcing fallback to a less secure method, or it might accept any device that has the shared login's cookie cached.

Group permissions add another layer of complexity. A single account with broad group permissions can access many resources. If that account is shared, any person using it inherits the full set of permissions. There is no way to restrict what a specific individual can do. The principle of least privilege is undermined. The control expects that each person's access is limited to what they need for their job. Shared logins make that impossible to enforce.

What the reader should do

If you are a defence supplier working toward CPCSC Level 1 compliance, start with a full account inventory. List every user account that has interactive access to the protected system. For each account, identify the account owner - the real person who is responsible for that credential. Any account that does not have a named owner should be disabled or assigned.



Next, check whether MFA enrollment is enforced on every account. Most modern systems allow you to require MFA for all users, but legacy accounts or service accounts might be exempt. Service accounts that run automated processes do not need MFA, but they also should not be used by people. If a human logs into a service account, that account becomes a shared login in practice.

Finally, conduct an access review at least quarterly. Look for accounts that have not been used recently, accounts with group permissions that are broader than necessary, and any evidence of credentials being shared. A simple way to detect sharing is to check for simultaneous logins from different IP addresses or locations. If the same account is logged in from two places at once, it is likely shared.

For organisations that rely heavily on third-party suppliers, consider a separate supplier portal with short-lived accounts. Each vendor employee gets their own account that expires after the project ends. This keeps the account inventory clean and ensures that each person's MFA is unique. The extra provisioning effort is small compared to the risk of a shared account being compromised.

The CPCSC MFA requirements are not just about the technology. They are about accountability. Unique user IDs give you the ability to trace actions back to a person. That traceability is what makes MFA meaningful. Without it, the second factor is just another shared secret.

One practical resource that many Canadian defence suppliers use is a checklist that maps each ITSP.10.171 requirement to the evidence that an auditor expects. For example, the material available through Hans Study provides a structured way to prepare that evidence,

including the specifics around account inventory and MFA enrollment. The checklist walks through each control point and explains what kind of documentation satisfies the requirement.

When you review your own environment, ask yourself: can I tell exactly who logged into my system at 2 AM last Tuesday? If the answer is no because the login was shared, you have a gap to close. Start by creating individual accounts for everyone who needs access, enroll each account with a unique MFA token, and remove the shared credentials. The process takes time, but it is one of the most effective steps you can take toward compliance.

And once you have unique IDs and MFA in place, keep the discipline. A new supplier request comes in, and the easiest path is to reuse an existing account. Resist that urge. The effort you save today becomes a compliance finding tomorrow. The Hans Study approach emphasises building evidence that lasts, not just ticking boxes for a single audit. That means every account has an owner, every owner has MFA, and every session is traceable.

Shared logins are a convenience that undermines security and compliance. For Canadian defence suppliers, the CPCSC MFA requirements make that trade-off explicit. The control expects unique user IDs because without them, MFA cannot do its job. Start your account inventory now, and treat every shared login as a risk to resolve, not a shortcut to keep.