

Multi-Factor Authentication (MFA) - Schedule CS-5

Effective Date: October 14, 2025 | Supersedes prior versions.

Service Summary

Service Provider shall provide Multi-Factor Authentication (“MFA”) services to reduce risks of unauthorized access to Client systems and data. MFA requires end-users to confirm their identity using a second factor beyond username and password, such as a push notification, mobile application prompt, or hardware token. MFA significantly strengthens account security but does not guarantee prevention of account compromise.

Scope of Services

- Deployment and configuration of MFA policies on supported platforms, including Microsoft 365 and other integrated services.
- Default MFA option provided via Microsoft Authenticator for accounts licensed under Microsoft 365.
- Enhanced MFA coverage, including non-Microsoft systems, VPNs, and third-party applications, provided through Duo Security, which is a licensed, fee-based service.
- Management of MFA enrollment, enforcement, and exception handling for Covered Users.
- Ongoing monitoring of MFA adoption and basic troubleshooting assistance.

Exclusions

- Responsibility for user compliance (e.g., failure to enroll, lost devices, or bypassing MFA prompts).
- Protection against attacks that exploit compromised endpoints (e.g., session hijacking, token theft, malware-infected devices).
- Coverage of applications or platforms not integrated with Microsoft Authenticator or Duo, unless expressly agreed in writing.
- Support for legacy systems or third-party tools that do not support MFA integration.
- Any guarantee that MFA will prevent all unauthorized access attempts, especially in cases of user negligence or advanced attack techniques (e.g., MFA fatigue attacks).

Client Responsibilities

- Ensure end-users enroll in MFA promptly and maintain control of their registered devices.
- Promptly notify Service Provider if an MFA device is lost, stolen, or compromised.
- Authorize enforcement of MFA policies across all supported accounts; failure to enforce MFA universally increases risk and is outside Service Provider’s responsibility.
- Maintain proper licensing for Duo MFA where purchased.

General Terms

- MFA is provided as a best-effort protective service. While MFA significantly reduces the likelihood of unauthorized access, no system is impenetrable. Even the most advanced authentication systems remain subject to bypass or compromise.
- Client acknowledges that MFA is one element of a layered security strategy. Service Provider strongly recommends implementing complementary safeguards – such as endpoint detection and response (e.g., Adlumin XDR), conditional access policies in Microsoft 365/Intune/Entra ID, DNS filtering, email security, and security awareness training – to achieve stronger overall resilience.
- All response times for MFA-related service requests are governed by the Service Level Objectives in Schedule A of the Master Service Agreement.
- Fees for this Schedule are billed in accordance with the Payment Terms of the Master Service Agreement. Required platform licensing is included in Service Provider’s standard service fees unless otherwise specified. Additional costs (e.g., optional hardware, custom configurations, or third-party integrations outside standard service) may apply and will be billed separately.