Enhanced Security Services - Multi-Factor Authentication

1 Overview of the Service

NTT will provide an additional layer of security by combining two or more independent credentials.

(a) Multi-factor authentication for supported interactive Operating System logins for NTT managed systems that Client has determined require multi-factor authentication. Note: Interactive operating system/application service accounts are counted in the multi-factor authentication license count.

(b) Multi-factor authentication for supported interactive application logins for systems that Client has determined require multi-factor authentication. Note: Interactive operating system/application service accounts are counted in the multi-factor authentication license count.

2 Client Responsibilities

(a) Operating systems must support multi-factor authentication. Operating systems that do not support multi-factor support are out of scope.

(b) Client is responsible for integration with Client applications.

(c) Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for the multi-factor authentication and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents) .

(d) Client must provide define specific groups or categories of accounts that will be subject to MFA.

(e) Client must identify all systems that require MFA.

(f) Client responsible for end user training of MFA.

(g) Procurement of mobile devices and installation of MFA application.

(h) Client must agree to the applicable user terms and conditions and secure its agreement from the end user.

3 Service Levels

NTT offers the following service levels for multi-factor authentication and the level must be selected as In Scope in the SOW otherwise all are out of scope.

(a) Standard

(b) Access

Service Tasks	Standard	Access
MFA Push capabilities for iOS and Android, Security Keys, Call Back, SMS, or Hardware Tokens.	✓	✓
User Self-Enrollment and Self-Management.	✓	✓
Assign and enforce security policies globally or per application or per user groups.	✓	✓
Enforce policies based on authorized networks.	✓	✓
Enforce policies based on users location.	✗	✓
Block The Onion Router (Tor) and anonymous networks.	✗	✓
Enforce device trust policies based on security health of laptops and desktops (out-of-date software, encryption, firewall, etc).	✗	✓
Enforce device trust policies based on security health of mobile devices (encryption, tampered, screen lock, biometrics).	✗	✓

Tasks legend:

(c) Tasks marked as ✓ are included in the service for the specified level.

(d) Tasks marked as ✗ are not included in the service for the specified level.

4 Supported Environments

(a) NTT managed client on-premises data center

(b) NTT managed private and public cloud

5 Out of Scope

(a) MFA requires the installation of an Authorization Proxy service on an existing Active Directory server within the environment. This requires an additional fee.

(b) Enhanced Security is not a standalone offer, and can only be included when standard security is in Scope in the SOW.

Service Specific Terms and Conditions

By selecting this service as in Scope in the SOW Client and its End User explicitly agreeing to abide by the terms and conditions found at Enhanced Security Services - Multi-Factor Authentication Terms. NTT reserves the right to change the provider and associated legal terms from time to time and Client agrees to abide by these terms.