SERVICE DESCRIPTION

Nile Enterprise Trust Service

1. Introduction and Purpose

This Service Description ("Service Description") defines the Nile Enterprise Trust Service ("Service").

Nile Enterprise Trust Service is an optional, premium add-on to the mandatory Core Nile Trust Service that is included within every **Nile Trust Service** deployment, providing advanced, identity-based Zero Trust security and microsegmentation across the enterprise LAN. It builds on Nile's Core Trust Service capabilities to enforce least-privilege access, contain lateral movement, and extend consistent Zero Trust within wired and wireless networks as well as traffic to/from external locations - data centers, cloud, and Internet.

Enterprise Trust Service follows the three foundational Zero Trust principles — never trust, always verify; identity-based least-privilege access; minimizing the impact of a breach by containing lateral movement. It adds AI-driven, context-aware enforcement and continuous assurance integrated with Nile's Autonomous Operations, enabling end-to-end Zero Trust with adaptive controls and real-time analytics.

Nile will provide and operate the Service in alignment with the scope, responsibilities, and assumptions defined herein. The customer ("Customer") is responsible for administration for the underlying Nile Access Service, providing the necessary security intent, identity sources, and integrations, and defining and managing how the Service is used within its environment.

By subscribing to this Service, Customer agrees to the terms outlined in this Service Description and acknowledges its responsibilities in ensuring the successful delivery and operation of the Service.

2. Service Scope

2.1 In-Scope Activities

Nile Enterprise Trust Service includes the following capabilities and functions, in addition to the Core Trust Service that is added to every Nile Access Service subscription:

Identity-Based Microsegmentation

- Microsegmentation for all users, IT endpoints, IoT devices, and application policy groups to support fine-grained policies, which are enforced natively in the Zero Trust Fabric.
- Software-defined security perimeters based on user and device identity, in addition to the Segment or IP/Subnet constructs.

Least-Privilege Policy

- Policy decisions that are based on identity, enforcing least-privilege access on every connection.
- Granular traffic service profiles to tightly control which protocols, and destination ports are allowed.

Fine-Grained East–West and North–South Enforcement

- Native, fabric-level enforcement of both East–West (lateral) and North–South (to data center, cloud, or Internet) traffic.
- Default-deny model extended beyond segment or IP/subnet based Policy Groups to include software-defined security perimeters that may be identity-based.

Continuous Identity Assurance and Device Validation

- Continuous verification of identity and device fingerprints to detect identity drift, or spoofing, for managed and unmanaged endpoints.
- Active device validation (for example, via SNMPv3/SSH/HTTPS) and automatic quarantine policy groups for non-compliant or rogue devices.

Universal Zero Trust with SSE and Security Integrations

- Native integration with Secure Service Edge (SSE) partners, including Palo Alto Networks, Zscaler, and Microsoft Entra, to extend consistent Zero Trust policy from the LAN to cloud, Internet, and private applications.
- Support for integration with third-party NGFW, NAC/RADIUS, and analytics tools for identity-based enforcement and exported policy logs.

Nile RADIUS Service

- Nile RADIUS Service is included with Enterprise Trust Service, providing EAP-TLS (secure, and certificate-based authentication) as well as EAP-PEAP (username/password) as part of Enterprise Trust enforcement.
- Nile also integrates with MDM’s like Intune and Jamf to ensure only compliant devices are onboarded.

Policy Management, Visibility, and Analytics

- Centralized policy definition using identity-, MAC/OUI-, and User, Device, and App groups with unidirectional policies.
- Per-policy logging and export for audit, compliance, and troubleshooting.
- Unified visibility into connected devices, identity, access decisions, and enforcement state via the Nile Portal.

Operations as a Cloud Service

- Enterprise Trust Service is delivered as a cloud-managed security service tightly integrated with Nile Access Service and the Zero Trust Fabric, managed via Nile's cloud platform.

2.2 Out-of-Scope Activities

The following activities and services are not included in the standard Nile Enterprise Trust Service unless explicitly contracted under separate agreements (for example, Professional Services, Nile Ready, Nile Propel, or similar):

- **Third-Party Security Tool Management** – Configuration or lifecycle management of third-party security tools (NGFW, SSE, SIEM, NAC, EDR, MDM, IdP), except for supported and documented integration points.
- **Endpoint Security** – Endpoint security (EDR/AV), OS patching, host firewalls, or mobile/desktop management.
- **Incident Response and Forensics** – Incident response, threat hunting, or forensics outside the Nile network and Trust Service scope.
- **Custom Development** – Custom application development, bespoke policy engines, or unsupported integrations.
- **Professional Services** – Assessments and migration or integration engagements such as Nile Ready, Nile Propel, or custom compliance assessments, which are available separately.

3. Deliverables

When purchased, Nile Enterprise Trust Service provides Customer with the following service deliverables:

- **Active Enterprise Trust Service Instance** – An active Enterprise Trust Service instance for each subscribed Nile tenant running on the Nile Zero Trust Fabric and cloud platform.
- **Configured Identity and Policy Framework**, including:
  - User, Device, and App policy groups and traffic service profiles.
  - Default-deny baseline policies and microsegmentation rules
- **Integrated Authentication and Identity Assurance** – Configuration of Nile RADIUS Service and identity source integrations as supported.
- **Zero Trust LAN Enforcement** – East–West and North–South policy enforcement in the fabric, including quarantine groups and continuous device validation.
- **Visibility and Logging** – Access to enforcement dashboards, device and identity inventory, and per-flow policy logs in the Nile Control Center, with export of policy logs to supported external tools.
- **Ongoing Cloud Operations** – Continuous monitoring, automated updates, and integration with Nile's AI-Ops and Autonomous Operations where applicable.

4. Responsibilities

4.1 Nile Responsibilities

Nile will:

- Design and maintain the Enterprise Trust architecture as part of the Nile Trust Service portfolio, including Zero Trust Fabric integration, the policy engine, and supporting cloud services.
- Host and operate the Enterprise Trust Service in Nile's cloud environment, including:
  - High-availability operation of Trust control components.
  - Software maintenance, security patches, and feature updates.
  - Back-end scaling and resilience aligned to Customer's subscribed Access Service and Service Package tier.
- Provide centralized management and visibility via the Nile Portal for Enterprise Trust policies, endpoint inventory, and enforcement telemetry.
- Implement and enforce Customer-defined policies across the Nile Zero Trust Fabric, including identity-based microsegmentation, device quarantining, and SSE forwarding as configured.
- Support integrations with documented third-party services with approved tech alliance partners.
- Provide customer support consistent with Customer's overall Nile Service offer.

4.2 Customer Responsibilities

Customer retains responsibility for the obligations below, whether fulfilled internally, by a trusted partner, or via separate Nile Professional Services:

a. Service Foundation

- Maintain an active Nile Access Service subscription and a deployed Zero Trust Fabric with Core Trust Service, as Enterprise Trust Service is an add-on to Nile's managed LAN service and is not sold as a standalone product.

b. Security Intent and Policy Definition

- Define security intent and policies, including:
  - Identification of user roles, device categories, application groups, and required communication flows.
  - Risk posture and any exceptions to default-deny behavior.
- Approve and review policy changes proposed by Nile or partners before activation in production.

c. Identity and Integration Readiness

- Provide and maintain identity sources and integrations, including supported IdPs, directory services, MDM/EMM, or NAC/RADIUS systems as applicable, along with required accounts, API tokens, and connectivity.
- Maintain licenses and support contracts for any integrated third-party tools (SSE, NGFW, IdP, SIEM, and similar).

d. Site and Endpoint Readiness

- Ensure correctly deployed Nile hardware and connectivity per Nile Access Service guidance, and proper power, cabling, and environmental readiness at each site (often achieved via Nile Ready or Design services).

e. Operations and Support

- Operate the internal help desk and user communication, including user-facing support, onboarding guidance, and communication around policy changes.
- Handle application-layer issues outside Nile's control.
- Provide reasonable cooperation in troubleshooting, including logs or information from systems not managed by Nile when required.

Failure to fulfill these responsibilities may impact the successful delivery and performance of the Service and may require Change Orders, schedule adjustments, or additional fees.

5. Assumptions

Nile Enterprise Trust Service is provided under the following key assumptions:

- Customer has, or will have, Nile Access Service deployed with the Zero Trust Fabric and Core Trust Service, which form the foundation for Enterprise Trust capabilities.
- Enterprise Trust Service is packaged as the Enterprise Trust tier of the Nile Trust Service, included with Secure and Assure service plans, and available via the appropriate Trust options in the Nile Service Catalogue.
- Customer identity infrastructure (directory/IdP, MDM, and similar) is in place, supported, and correctly licensed.
- Sites are Nile-managed campuses,branches, or venues using the Nile Zero Trust Fabric; extension to other domains (for example, data center, cloud, or WAN) occurs via SSE/NGFW integration or Nile Edge Service where applicable.
- Customer has an active subscription to Nile Enterprise Trust Service and term, as documented in the relevant order or commercial agreement.

6. Exclusions

Enterprise Trust Service is subject to the following exclusions and limitations, in addition to those in the Nile Master Services Agreement and pricing guide. Unless explicitly stated in an Order Form, Statement of Work, or other written agreement, Nile will not:

- Enforce policy on traffic that does not traverse Nile-managed infrastructure, except where governed by integrated SSE/NGFW policies outside Nile's control.
- Sell or provision Enterprise Trust Service as a standalone product without an active Nile Access Service subscription and Core Trust Service.

- Guarantee achievement of specific certifications or regulatory approvals; Nile provides controls and evidence to support Customer compliance efforts but does not guarantee compliance outcomes.
- Assume responsibility for outages or limitations in third-party services (IdP, SSE, NGFW, SIEM, and similar) on which certain functionality depends; those services are subject to their own vendors' availability, performance, and feature sets.
- Support policy complexity or bespoke segmentation beyond the scale and use-case boundaries documented in the Nile Trust Service scope without an optional, separately contracted Professional Services engagement.
- Assume responsibility for delays or issues caused by Customer, third-party vendors, or factors outside of Nile's reasonable control.

All Services and Deliverables are non-transferable and provided solely to the Customer entity purchasing the Services and covered sites; the Service may not be resold or transferred except as permitted in the governing agreement.

7. Fees and Payments

- Nile Enterprise Trust Service is billed on a subscription basis, co-termed to the Customer's Nile Access Service contract. Specific pricing, term length, and metrics are defined in the applicable pricing documents and Customer order.
- Fees may depend on factors such as the number of active endpoints, the number of covered sites, the fabric design model, and included lifecycle elements (for example, data retention and training), as described in the pricing documents.
- Estimates (for example, a Rough Order of Magnitude) are based on initial Customer inputs; final pricing is determined after design validation and any required site discovery. If the final implementation differs from initial assumptions, a Change Order may be required and fees may be adjusted accordingly.
- Material changes in scope (for example, additional regions, accelerated timelines, or expanded endpoint counts) may require incremental capacity, which can be handled through change orders that adjust service quantities.

Service Name
• Nile Enterprise Trust Service

- If the Customer is purchasing the Services directly from Nile, payment obligations are governed by the "Payment Obligation" section of the **Terms and Conditions**. Fees for Services purchased through an authorized reseller or distributor shall be paid directly to such authorized reseller or distributor.