Service Description
Cisco Support National – Signature

This Service Description is part of the Services Agreement (as defined in the Services Guide) and describes various Services that Cisco will provide to You. Capitalized terms, unless defined in this document, have the meaning in the Services Guide.

1. Summary

Cisco Support National – Signature provides You with access to a team of authorized personnel who possess the necessary government clearance to provide the Service. This Service provides support in alignment with the requirements of the respective country's public sector and relevant national security programs. Cisco service requests and correspondence data provided to Cisco for the purpose of delivering the Cisco Support National – Signature Service are not subject to international data transfers and are stored on a network with restricted access controls.

2. Cisco Responsibilities

Cisco will provide the features described below, as selected and detailed on the PO for which Cisco has been paid the appropriate fee.

Capabilities	Features	Airgapped
Trusted Support	Support Access	•
	Software Updates and Maintenance Releases	•
	Support Communities	•
	Solution Level Support	•
	Prioritized Case Handling	•
	Case Expedition, Risk Mitigation, and Resilience	•
	Periodic Service Reviews	•
	Systematic Root Cause Investigation	•
Trusted Support Software	Smart Account Guidance	•
	Setup Configuration Support	•
	Health, Updates, and Change Support	•

2.1 Trusted Support

(A) **Support Access**

Cisco will provide access to Cisco Support Teams 24 hours per day, 7 days per week to assist with Product use, configuration and troubleshooting issues by online and phone. Cisco's initial response time will be as follows:

Initial Response Time	Signature
Severity 1	15 minutes
Severity 2	30 minutes
Severity 3	1 hour
Severity 4	1 hour

(B) **Software Updates and Maintenance Releases**

For applications, licenses, and hardware OS, Cisco will provide work-around solutions or patches for reported Software problems (when available), and You will have access to Software Releases, as applicable.

(C) **Support Communities**

Cisco will provide Cisco-moderated communities where Cisco experts answer FAQs, hold expert-led Q&A forums, and provide Product and Service recommendations.

(D) **Solution Level Support**

Cisco will provide Solution Level Support, which includes centralized expertise and issue management across a solution of Cisco and Cisco approved third-party provider ("Solution Alliance Partner") products. Solution Level Support applies to solutions comprised of Cisco and Cisco approved Solution Alliance Partners products, where You maintain: (1) Cisco Solution level support on all Products (where available) and (2) an appropriate level of technical support on all Cisco Solution Alliance products used in the solution.

- Access to a team of solution experts who act as a primary point of contact who will either actively manage the issue to resolution by Product experts or, to the extent allowed by Solution Alliance Partners, coordinate Your actions to drive issue resolution.

(E) **Prioritized Case Handling**

Cisco will prioritize Support cases for Cisco Support National - Signature.

(F) **Case Expedition, Risk Mitigation, and Resilience**

Cisco will provide management of support cases and risk through:

- Operational support for the management and resolution of Severity 1 and Severity 2 cases.
- Coordination with Customer and Cisco stakeholders.
- Management of support cases and RMA requests to closure, with escalation as necessary.
- Highlighting of technical debt to facilitate prioritization and remediation of aging components or configurations.
- Vulnerability assessments to identify and address security or stability concerns before exploitation.
- Evaluation of the impact of planned changes to assess how modifications may affect system stability.
- Delivery of maintenance window support:
    - Reactive Maintenance Windows (RMW): Coordinated with You to address urgent changes necessary to resolve Service-impacting issues identified in Cisco support cases.
    - Scheduled Maintenance Windows (SMW): Your initiated maintenance periods not directly linked to an open Service-impacting Cisco support case. Cisco reserves the right to limit SMWs to twelve (12) per annual contract term, as defined by the Services Term.

(G) **Periodic Service Reviews**

Cisco will discuss with You supported cases, known errors, post-incident operational improvements, operational abnormalities and trends, and analytics and KPI reporting.

(H) **Systematic Root Cause Investigation**

Cisco will provide insights for on-premise Software to:

- Identify underlying systemic weaknesses that could cause recurring incidents.
- Map interdependencies to identify cascading effects. This feature is limited to devices related to the specific issue(s).
- Review historical patterns to highlight recurring issues that may require architectural or procedural changes.
- Document findings comprehensively, building a knowledge base to prevent recurrence.
- Facilitate problem resolution for technical issues that You report.
- Provide assistance, troubleshooting, or remediation for Your Network.

2.2 Trusted Support – Software

Trusted Support - Software provides proactive support, expert guidance, and actionable advice to minimize risk and enable knowledge of Your Network.

(A) **Smart Account Guidance**

Entitlement guidance for Smart Account setup and Software license activation.

(B) **Setup Configuration Support**

Includes guidance for initial installation and deployment of the Application Software, deployment of Software updates and migration, and support associated with integrating the Application Software into Your IT environment.

Examples include:

- Guide initial installation and deployment pertaining to the Application Software.
- Make recommendations on leveraging best practice guides, training materials, and/or suggesting process changes to better achieve desired outcomes.
- Provide best practice training for Your help desk personnel on processes and Application Software features.
- Conduct periodic Cisco system risk evaluation for on-premises deployments (at Cisco's discretion).

(C) **Health, Updates, and Change Support**

Cisco provides ongoing support activities designed to help you maintain a stable, well-performing deployment and prepare for software updates and planned changes. These include:

- Periodic technical health check reviews to:
  - Assess and recommend changes to the Software configuration and provide technical guidance.
  - Compare progress to date against goals.
  - Address limitations or influences related to IT and Infosec adoption plan.
  - Guide deployment of Software updates and migration.
- Availability Advisories to provide safeguards against known issues and changes that may affect operation and availability of the Application Software.
- Planned change impact guidance for planned Product changes that may affect availability of the Application Software or its feature set.
- Semi-annual consultation to help plan for upgrades, expansion, and migration for any necessary deployment growth.
- Annual summary to include support case trend analysis, Software configuration review, and recommendations for any changes.

3. Customer Responsibilities

a) Designate an authorized point of contact with the appropriate authority and clearance level to coordinate all aspects of the Services.

b) Define and maintain security, incident management, and handling procedures, and provide relevant documentation required for Cisco to operate within the defined compliance boundary.

c) Establish and communicate environment readiness requirements, including access constraints, connectivity limitations, and any conditions for operating within controlled environments.

d) Facilitate all data exchange and support interactions within Airgapped or isolated environments, including providing required diagnostic data through approved offline or controlled transfer methods.

e) Provide asset classification, prioritization, and permissible network activity guidelines to support effective triage, troubleshooting, and incident response.

f) Ensure facilities, systems, and personnel are prepared for service delivery, including granting authorized and secure access to in-scope assets within the defined boundary.

g) Coordinate and manage any required onsite activities, including advance scheduling and ensuring

compliance with site-specific security and access protocols.

h) Report critical issues (Severity 1 and Severity 2) through defined channels and support timely troubleshooting, including performing initial diagnostics where required.

i) Review and act on incident updates and recommended mitigations in a timely manner, particularly where required to maintain system availability and security posture.

j) Perform required onboarding and transition activities to enable service activation within the controlled environment.

k) Maintain responsibility for overall network design, security, and compliance posture, including decisions related to implementation of Cisco recommendations.