GOVERNMENT OF INDIA
(Ministry of Home Affairs)
COMMUNICATION & IT DIRECTORATE
CENTRAL RESERVE POLICE FORCE
EAST BLOCK-7, SEC-1, R.K. PURAM, NEW DELHI-110066
(Email:- comncell@crpf.gov.in Tele/Fax:011-26109038)

No. B.V-7/2024-25-C-(NAC)-Q Dated, the 2 June'2025

To

1. The DsG: AR, BSF, CISF, ITBP, NSG, SSB and BPR&D
2. Director, DCPW

Subject: Regarding QRs/TDs of "NAC (Network Access Control)"

I am directed to refer on the subject mentioned above and to say that the QRs/TDs of **"NAC (Network Access Control)"** has been approved by the DG CRPF after deliberation and recommended by CAPFs sub-group and experts from DCPW.

Encl:-As above

{Harjinder Singh}
DIG (Communication)
Communication & IT Branch
Directorate General C R P F

No. B.V-7/2024-25-C-(NAC)-Q Dated, the 2 June'2025

Copy to:-

2. Mrs. Sugandhi, Technical Director, North block, MHA with request to upload the QRs/TDs of **"NAC (Network Access Control)"** on MHA website (e-mail ID: mpsugandhi@nic.in).

Encl:-As above

{Harjinder Singh}
DIG (Communication)
Communication & IT Branch
Directorate General C R P F

QRs/TDs of NAC

S.N.	Specifications	Trial Directives
The proposed solution shall meet the below specifications. Any hardware/software/licenses required to enable the functionality shall be provided from Day 1		
A	**Device Profiling and Visibility**	
1	Automatic detection and categorization of endpoints for security and audit demands, regardless of device type.	Verification with OEM Tech brochure and Console Software
2	Stored profiling data should identify device profile changes and dynamically modify authorization privileges. *For example, if a printer appears as a Windows laptop, the system can automatically deny access. should support Load balancing for profile scans and Scheduled Subnet scans*	Verification with OEM Tech brochure and Console Software
3	Support passive device profiling methods such as DHCP, Span Ports, HTTP User-Agent, MAC OUI / Finger Printing and TCP SYN-ACK handshakes	Verification with OEM Tech brochure and Console Software
4	Support active device profiling methods such as SNMP, Subnet Scan, SSH, Sflow/RSPAN, WMI and NMAP Scan	Verification with OEM Tech brochure and Console Software
5	Internal device fingerprint dictionaries that provide a way to automatically or manually update periodically. Capable to define custom fingerprints for wired and wireless devices	Verification with OEM Tech brochure and Console Software
6	Offer a comprehensive dashboard to see the total number of endpoints, and the number by category, family and device type.	Verification with OEM Tech brochure and Console Software
B	**Authentication, Authorization and Accounting (AAA)**	
1	Integrated scalable AAA services (authentication, authorization, and accounting) including access policy management with a complete understanding of context, such as user's role, device type, location, time of day etc.	Verification with OEM Tech brochure and Console Software
2	User and device authentication based on 802.1X, and Web Portal access methods across multi-vendor wired networks, wireless networks, and VPNs	Verification with OEM Tech brochure and Console Software
3	Usage of multiple authentication protocols concurrently, such as PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, and EAP-PEAP-Public.	Verification with OEM Tech brochure and Console Software
4	Must support RADSEC protocol to support RADIUS datagrams over TCP and TLS. Should be able to work on all major OEM network switches.	Verification with OEM Tech brochure and Console Software
5	Must be supplied with fine-grained control using attributes from multiple identity stores, such as Microsoft Active Directory, Kerberos, LDAP-compliant directory, Open Database Connectivity (ODBC)-compliant SQL database, token servers, and internal databases across domains within a single policy from day one	Verification with OEM Tech brochure and Console Software

S/No	Specifications	Trial Directives
6	Non-802.1X devices (such as printers, IP phones, IP cameras and IOT devices) can be identified as known, based on the presence of their MAC addresses in database, or unknown upon connecting to the network.	Verification with OEM Tech brochure and Console Software
7	Integrated TACACS+ server for secure authentication of device administrators, operators etc. with varied privilege levels. It should keep a track of the changes made by the logged-in user.	Verification with OEM Tech brochure and Console Software
8	Customizable Reporting with manual or scheduled reports in PDF/CSV formats, inventory dashboard showing details of learned devices, real-time monitoring of access requests and events, proactive alerts through Email	Verification with OEM Tech brochure and Console Software
9	HTTP/RESTful API's, syslog messaging and Extensions capability to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management	Verification with OEM Tech brochure and Console Software
10	Mobile Device Management Integration to fetch information such as device manufacturer, model, OS Version, Jail-broken, presence of any black-listed application, MDM Agent installation status etc. and use this information in access policies	Verification with OEM Tech brochure and Console Software
11	API Integration with helpdesk software allowing dynamic creation of problem tickets of any network triggered policy breaches	Verification with OEM Tech brochure and Console Software
12	Inbuilt utilities for interactive policy simulation and monitor mode for assessing the policies before applying to the production network	Verification with OEM Tech brochure and Console Software
13	Process inbound threat-related events (which are Syslog events received from any third-party vendor device, such as Firewall, SIEM) and perform enforcements and actions based on the defined enforcement policies and services.	Verification with OEM Tech brochure and Console Software
14	Must have Multi domain and multiple AD and user database support for user information	Verification with OEM Tech brochure and Console Software
15	All the user machines must be evaluated before allowed on the network and thus must only deploy with a secured IEEE 802.1X architecture	Verification with OEM Tech brochure and Console Software
C	**Guest Access Management**	
1	Easy-to-use guest management solution for visitors, contractors, partners, Auditors etc. on wireless and wired networks using any type of device.	Verification with OEM Tech brochure and Console Software
2	Guest access through captive portal with extensive branding and customization including company logos, visual imagery and optional advertisements with multimedia content to extend organization's messaging	Verification with OEM Tech brochure and Console Software

S/No	Specifications	Trial Directives
3	Captive portal (Responsive Design to support different screen size) should have mobile device awareness to automatically size for smart phones, tablets and laptops	Verification with OEM Tech brochure and Console Software
4	Guest self-registration through the web portal, delivering username and password directly to the visitor's Web browser, or sent via email or SMS.	Verification with OEM Tech brochure and Console Software
5	Sponsor-based approval workflow to enable an internal employee to approve guest account before guest is allowed to access the network	Verification with OEM Tech brochure and Console Software
6	Customize guest access privileges to enforce bandwidth limits, access to specific resources, length of connections and set automatic account expiry after a specified number of hours or days	Verification with OEM Tech brochure and Console Software
7	Guest portal shall have an option to accept logins based on AD, RADIUS, IDAM or Social sites	Verification with OEM Tech brochure and Console Software
8	Third-party integration providing customizable workflows using rest-based API's for delivering streamlined registration and payment system integration	Verification with OEM Tech brochure and Console Software
D	**Personal Device (BYOD) Management**	
1	Automatically configure and provision mobile devices such as Windows, macOS, iOS, Android, Chromebook, and Ubuntu, enabling them to securely connect to enterprise network. Support for at least (*No of Users defined by User Department*) users on day one. Each user can have up to two devices and support Sponsor approval required option for Onboarding.	Verification with OEM Tech brochure and Console Software
2	Offer built-in certificate authority (CA) to secure device onboarding without requiring the implementation of an external CA or make changes to an internal public key infrastructure (PKI). In case for some reason any OEM unable to provide inbuilt CA then can provide it externally, however from day one. should work as a Root or Intermediate CA and support Self-help portal for certificate management	Verification with OEM Tech brochure and Console Software
3	Ensure rapid revocation and deletion of certificates for specific mobile devices if a user leaves the organization or the mobile device is lost or stolen.	Verification with OEM Tech brochure and Console Software
4	Support Online Certificate Status Protocol (OCSP)	Verification with OEM Tech brochure and Console Software
5	Capable to define the number of devices that can be on-boarded per user and validity of their certificates	Verification with OEM Tech brochure and Console Software

S/No	Specifications	Trial Directives
6	Automatic device certificate provisioning/installation with sponsor approval required option for onboarding	Verification with OEM Tech brochure and Console Software
7	Certificate Provisioning must work even after failover of its nodes	Verification with OEM Tech brochure and Console Software
8	Must support Oauth and SAML 2.0 Identity Provider, which allows seamless single sign-on (SSO) to the cloud or on-premise applications.	Verification with OEM Tech brochure and Console Software
9	Must support multiple multi-factor authenticators (MFA/2FA)	Verification with OEM Tech brochure and Console Software
10	Should support Secure certificate-based onboarding and Automatic device certificate provisioning / installation	Verification with OEM Tech brochure and Console Software
E	**Endpoint Posture Checking**	
1	Support Perform advanced endpoint posture assessments to ensure organization's compliance is met before devices connect	Verification with OEM Tech brochure and Console Software
2	Support the following operating systems and versions: Microsoft Windows 10 and above, Apple mac OS 10.10 and above	Verification with OEM Tech brochure and Console Software
3	Support Users of unhealthy endpoints that do not meet compliance requirements, should receive a message about the endpoint status and instructions on how to achieve compliance	Verification with OEM Tech brochure and Console Software
4	Support Endpoint posture and health checks should include Installed Applications, Antivirus, Firewall, Network Connections, Processes, Patch Management, Peer to Peer applications, Virtual Machines.	Verification with OEM Tech brochure and Console Software
5	Support to persistent agent for operating system to provide nonstop monitoring of the end point with automatic remediation and control	Verification with OEM Tech brochure and Console Software
6	Support Offer web-based dissolvable agent for endpoint compliance check of personal and non-IT-issued devices	Verification with OEM Tech brochure and Console Software
7	Must support detect multiple network interfaces and Control it	Verification with OEM Tech brochure and Console Software
8	The solution must ensure standard based Zero Trust access network security framework with 24/7 network policy compliance checking and enforcement.	Verification with OEM Tech brochure and Console Software
F	**Management and Reporting**	
1	Predefined templates for reporting must be available	Verification with OEM Tech brochure and Console Software
2	Solution must have built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.	Verification with OEM Tech brochure and Console Software
3	Solution must collect and keep forensic evidence on any unauthorized access activity within the network as follow: Event timestamp, network events in sequence, host info, IP address, MAC address, switch info etc.	Verification with OEM Tech brochure and Console Software

S/No	Specifications	Trial Directives
4	Solution must support capability to generate report for hardware (Memory, RAM, HDD, Peripheral devices, etc.), All installed software with version, Open ports, Service Running, Process Running and application inventory across managed extended enterprise.	Verification with OEM Tech brochure and Console Software
5	Solution must be able to display information notifications in an interactive manner viz. bubble notification, email, etc.	Verification with OEM Tech brochure and Console Software
6	The NAC solution should be able to integrate with Nextgen SIEM and other SOC components.	Verification with OEM Tech brochure and Console Software
7	The proposed NAC solution should provide user-friendly policy management (policy search, policy updates, import/ export policies, etc.)	Verification with OEM Tech brochure and Console Software
8	A reporting option must be available to provide a method for delivering validated templates to unique requirements in a timely manner.	Verification with OEM Tech brochure and Console Software
9	Understanding trends, compliance and forensic analysis requires the ability to generate reports on data from selectable time frames in the past as well as on current data i.e. Specific date and time range	Verification with OEM Tech brochure and Console Software
10	In order to provide the information needed to make decisions and minimize data overload reporting systems must provide robust filtering options.	Verification with OEM Tech brochure and Console Software
11	Must have support for notifications via Email	Verification with OEM Tech brochure and Console Software
12	Web-based user interface that simplifies policy configuration, monitoring and troubleshooting	Verification with OEM Tech brochure and Console Software
G	**Capabilities with Existing Unmanaged Switches**	
1	The Proposed NAC solution should able to detect the endpoint at the instant it connects to Customer network	Verification with OEM Tech brochure and management Software
2	The Proposed NAC solution should able to restrict communication to a non-compliant device which is connected to a hub/unmanaged switch, while another compliant device which should remain functional.	Verification with OEM Tech brochure and management Software
H	**Capability of building complete device inventory & context.**	
1	Solution should maintain an up-to-date/centralized inventory of authorized devices connected to network and authorized devices enabling the network	Verification with OEM Tech brochure and management Software

S/No	Specifications	Trial Directives
2	Solution must provide true-up enterprise endpoint data with complete device inventory & context in automated manner.	Verification with OEM Tech brochure and management Software
3	Solution must be able to provide compliance for Hardware properties on windows like Hardware Computer, Disks, Monitors, Motherboard, Network Adapter, Physical Device, Physical Memory, Plug and Play Device, Processor, etc.	Verification with OEM Tech brochure and management Software
4	Solution must automate the inventorying of IP-connected assets across extended enterprise networks along with detailed information of hardware viz. Disks, Monitors, Motherboard, Network Adapter, Physical Device, Physical Memory, Plug and Play Device, Processor, etc. Pinpoint the real-time location of all IP-connected things, Continuously and accurately assess all IP-connected devices.	Verification with OEM Tech brochure and management Software
I	**Requirement Summary**	
1	The solution should be based Hardware appliance. The solution must support minimum 500 (Number defined by User Department) endpoint support from Day-1.	Verification with OEM Tech brochure and management Software
2	The solution shall support minimum 200 authentications per second for 802.1x/RADIUS/TACACS+/Guest and minimum 50 clients/second for endpoint posture checking	Verification with OEM Tech brochure and management Software
3	Licenses supporting minimum 500 (Numbers decided by User department) concurrent sessions for AAA, Endpoint posture check, Guest access, (Numbers decided by User department) Endpoint Profiling and (Numbers decided by User department) BYOD devices from day-1. Solution Should scalable as per user department.	Verification with OEM Tech brochure and management Software
4	5-Year 24x7 Hardware and Software Warranty with perpetual / subscription licenses.	Verification with OEM Tech brochure and management Software
J	**OEM and Product Eligibility/Compliance**	
1	The solution shall be Common Criteria certified for network access control (NAC) solution, under both the Network Device collaborative Protection Profile (NDcPP) and the Extended Package for Authentication Servers modules. The certificate shall be attached as reference	Firm will provide OEM Certificate.
2	OEM shall have R&D facility in India; if required site visit shall be arranged	Firm will provide OEM Certificate
3	AAA shall be offered with minimum five years hardware warranty with 24X7 OEM direct support along with software updates/upgrades	Firm will provide OEM Certificate

S/No	Specifications	Trial Directives
4	**Optional:** On Site OEM certified Engg. (Be decided by user department)	Firm will provide OEM Certificate

21/5/25

(Hanif Choudhury)
AC(Exe), CISF

(Ujjwal Kumar Singh)
AC(QR), CRPF

(Major Atul Sharma)
NSG

21/5/25

(Prem Narain)
DC(Comn),SSB

(Vimal Singh)
DC(IT), CRPF

(Sunil Kumar Singh)
DC(Comn),CRPF

(Vivek Kr Gupta)
AD, DCPW

(Lt. Col V.P.Singh)
Assam Rifles

(Koushik Choudhury)
Sr. Director (IT), NIC

Pandey

(Rajesh Pandey)
Comdt (Tele), ITBP

(S.K. Sastri, Comdt)
BSF

(P.C.Jha)
DIG(Comn), CRPF

(Vijay Kumar)
IG, CRPF

(Syed Mohammad Hasnain)
IG (Comn& IT), CRPF

(Vitul Kumar, IPS)
SDG (OPS), CRPF

✓

Approved/~~Not Approved~~

(Gyanendra Pratap Singh, IPS)
DG, CRPF