

Network Device Interpretation # 202420

Local IP address for Administrative Access

Status: *Active* *Inactive*

Date: *2-Dec-2024*

End of proposed Transition Period (to be updated after TR2TD process): *1-Jan-2024*

Type of Change: Immediate application Minor change Major change

Type of Document: *Technical Decision* *Technical Recommendation*

Approved by: *Network iTC Interpretations Team* *Network iTC*

Affected Document(s): *NDcPPv3.0, ND_SD_3.0e*

Affected Section(s): *FIA_AFL.1, FMT_SMF.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

A product was previously evaluated against NDcPP v2.2e. The only supported mechanism for admin authentication (both local and remote) is passwords, and account locking per FIA_AFL.1 is enforced on remote admin access. Per the App Note for FMT_SMF.1 in NDcPP v2.2e, item (c) (“Use of a dedicated Ethernet port...”), local administrators are supported via a dedicated Ethernet port using HTTPS, and account locking is not enforced on admin access using this port. This implementation satisfies the requirement in the App Note for FIA_AFL.1 that “the TOE ensures that authentication failures by remote Administrators cannot lead to a situation where no Administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).” Guidance documentation provides direction for local admin access via the dedicated Ethernet port using a local IP address.

We are planning a new evaluation of the product against NDcPP v3.0e. The product maintains all the functionality described above. The NDcPP local/remote administration requirements are largely consistent between the 2 NDcPP versions, except that local administration is optional in NDcPP v3.0e. However, the App Note for FMT_SMF.1 in NDcPP v3.0e no longer includes item (c) regarding a dedicated Ethernet port. The intent of this change is not apparent, especially since the App Note for FIA_AFL.1 still contains the “local logon which is not subject to blocking” text.

Please clarify whether:

- A dedicated Ethernet port using a local IP address still qualifies as local administrator access.

- Not enforcing account locking on local admin access still satisfies the requirement in the App Note for FIA_AFL.1 that Administrator access is always available.

Resolution:

The NIT disagrees with the premise that a dedicated Ethernet port using local IP addressing still qualifies as local administrator access in NDcPPv3.0e. Assignment of an IP address indicates remote access. Only directly wired connectors (e.g., RS-232) are intended to be classified as 'local' and it is optional to implement in NDcPPv3.0e.

Rationale:

see Issue section

Further Action:

None

Action by Network iTC:

None