



**Trusted Network Connect (TNC) Clientless Endpoint Security Profile
FAQ
May 2009**

Q. What is the purpose of the Clientless Endpoint Security Profile?

A. The TNC Clientless Endpoint Support Profile allows a network administrator to secure devices that attach to the network but lack a TNC client (health checking software). Examples include printers, VoIP handsets, and guest laptops. These devices, which are quite common in the enterprise, create a management headache when deploying Network Access Control (NAC) because they do not or cannot participate in the NAC protocols. The TNC Clientless Endpoint Support Profile provides a standard methodology for authorizing and monitoring these systems to ensure interoperability and seamless integration and security for all connected devices in a TNC architecture.

Q. How does this improve things for networks that use the TNC protocols?

A. The TNC Clientless Endpoint Support Profile allows network administrators to automate the management of non-TNC systems on a TNC-enabled network. These devices can now be automatically identified, inventoried, and monitored. This is a big improvement over previous methods where ports were blocked open to allow printers to access the network. By securing all systems on the network, network operators will no longer have to deploy static overrides to deploy network devices such as printers, copiers, access card readers etc. The TNC Clientless Endpoint Support Profile will provide a lower cost of operation and improved security posture when integrating systems lacking a TNC client.

Q. How does the Clientless Endpoint Support Profile work?

A. The profile describes how key components of the TNC architecture should work together to secure networks when clientless endpoints attempt to connect. The profile describes several ways to handle clientless endpoints. Here's a description of one common technique: a Consultation-Based Decision.

The process starts when a Policy Enforcement Point (PEP) such as an Ethernet switch detects a clientless endpoint connecting to the network. The PEP uses techniques described in the profile to identify the endpoint and send this identification information (e.g. a MAC address) to a Policy Decision Point (PDP). The PDP consults administratively configured policy to determine whether the endpoint should be allowed (e.g. is it a known device in its proper location) and sends the resulting access control decision to the PEP. Depending on the sophistication of the network and the level of security desired, the endpoint may be scanned before admission to the network and monitored after admission to ensure that its behavior is appropriate for its device type and identity. If anomalous behavior is detected, the device can be quarantined or an alert can be raised.

Q. Are there products supporting the Clientless Endpoint Support Profile?

A. Because the Clientless Endpoint Support Profile is based on existing industry best practices, many existing switches and NAC servers already comply with the basic, required elements of the profile, which standardize "MAC authentication."

In fact, many vendors already support the more advanced functions of the Clientless Endpoint Support Profile, such as storing information about clientless endpoints into a Metadata Access Point (MAP) to enable monitoring.

Q. Are any other standards involved or supported?

A. The TNC Clientless Endpoint Support Profile builds upon existing TNC standards (IF-PEP) as well as IEEE 802.1X and IETF RFC 3580.

Contact: Anne Price, TCG market communications
anne@prworksonline.com
1-602-840-6495