

PROTEXX



## Device Authentication

Secure Access for First Responder Networks

Desktop Alert  
Desktop notification made easy  
<http://www.desktopalert.net>

### A Valuable Tool for Eliminating Unauthorized File and Device Access

**Enterprises, SMB's and Federal and Local government agencies** seeking to improve the effectiveness of their Internet security should consider the use of *device authentication* capabilities provided by **Protexx**. *Device Authentication* is a relatively new security capability that provides the most cost-effective layer of security available today to any comprehensive security architecture. Most network authentication solutions presently identify the user through *passwords, tokens, smart cards, or biometrics*. While these techniques can provide effective identification and authentication of an *individual* user, a comprehensive security policy must also identify the device employed by that *Authenticated user*.

#### *What Is Device Authentication?*

*Device Authentication* is a solution that enables an organization to manage the user and the device; not just the user. It is a *second layer of authentication*, ensuring that only a specific *pre-authorized* device operated by specific *pre-authorized users* can access the network. **Separately, neither one can gain access!**

This means that even if a *password* or *token* has been compromised, the network is still protected, as long as the *Authorized machine* is not used. It also assures that confidential data is never exposed because *Un-Authorized devices* are not allowed onto a network, even when operated by an *Authorized user*. So, for example, an *Authorized user* at work cannot access when using an *Un-Authorized PC* at home.

#### *What are the security benefits of Device Authentication?*

***Device Authentication* provides the following benefits by enhancing network security favorable to a return on investment:**

- It further enhances the network's security by adding another layer of protection to the overall network security architecture. *Device Authentication* allows only *Authorized* users, employing previously *authenticated* and then enrolled *devices* to enter the network and access data. This permits organizations to manage **Mobile O/S's, Mobile security** and **Mobile applications**; all synchronized to the *user* with device policies.
- *Device Authentication* integrates the secure identification of **Authorized desktops, laptops** and other **mobile** devices into a comprehensive organizational security strategy at a very reasonable cost.
- *Device Authentication* is particularly effective for securing remote access by **Mobile users** and **Home Office users** who must access the network through a **VPN** or other remote connection utilizing a *Protexx Remote VPN*.
- *Device Authentication* can be a strategic enabling technology for **Enterprises**, for **SMB's**, for **e-Government** and other agency applications where the control of the device coupled with the control of the *user* is an important security concern.