

DeviceID™

Ensure That Only Trusted Devices Access the Enterprise

- Establish which endpoints are trustworthy through a unique device identification process
- Validate device identity and policy compliance as factors for VPN authentication
- Ensure that only policy-compliant, corporate-issued or -authorized machines access the network
- Require use of the iPassConnect™ universal client and the Endpoint Policy Management™ service for enforcement of security and connectivity policies



Your corporate IT staff has serious trust issues — and rightfully so. Deceptive practices such as password theft, identity spoofing and replay attacks leave IT professionals wondering who is on the corporate network at any given time. Even the most confident IT managers are left wondering whether it's possible to prevent unauthorized devices from accessing the enterprise.

Strong multi-factor authentication is the best approach to ensuring that only known individuals access the corporate network. However, point solutions, such as tokens, only provide a stronger set of credentials for network access which is only a small part of establishing trusted connections. Until now, each new layer of security has come with additional costs, administration overhead, and weaknesses that can be easily taken advantage of to circumvent security policies.

Fortunately, there's a new way to address these challenges through multi-factor authentication and VPN enforcement. It's the DeviceID service. It's innovative, affordable and delivered by iPass — a trusted leader in enabling secure connections without compromise.

STRENGTHEN NETWORK SECURITY WITH MULTI-FACTOR AUTHENTICATION

The DeviceID service helps IT managers to create and enforce access policies that work to ensure only corporate-authorized devices gain network access. Patented, software-based authentication technology based on a fault-tolerant architecture, lets you know with certainty which devices are requesting access to your enterprise network. With its unique ability to distinguish company owned assets from personal devices or completely unknown computers, DeviceID can play a valuable role in identity, access and policy management.

Dynamic Machine Interrogation: Identifies machines by checking different hardware attributes for each authentication request, protecting against replay attacks, reverse engineering and spoofing.

Encryption of "Digital Fingerprint": Hardware attributes are translated into a "digital fingerprint" of unique device identifiers that is encoded before transferring it over a secure channel and storing the results in protected authentication servers for comparison and validation.

Strong Two-Factor Authentication: Combines device identification with a user name and password to restrict network access to authorized devices and authenticated users. No additional expensive hardware or complex software-based solutions required.

UNIVERSAL POLICY ENFORCEMENT

The DeviceID service takes policy enforcement to a new level. It helps you establish the trust-worthiness of endpoint devices by confirming device properties prior to allowing VPN authentication. When configured to require the use of the iPassConnect universal client and the Endpoint Policy Management service, DeviceID can ensure that enterprise security systems are used in a policy-compliant manner before granting network access.

Through DeviceID, IT gains the flexibility of establishing simple or sophisticated policies and controlling VPN access to the corporate network based on policy compliance. Whether you choose basic two-factor authentication that restricts use of specific devices to defined users or prefer to institute more complex policies that require devices run up-to-date corporate-approved security software, DeviceID puts you in control. By integrating with DeviceID, the following implementation options leverage device authentication to provide different levels of endpoint lockdown and policy enforcement:

Trusted connections. No compromises.





Require use of iPassConnect: Ensure personal firewall and anti-virus software are running prior to allowing VPN access. Network connection is only allowed through iPassConnect and is disabled if endpoint software is not in use continuously.

Apply Endpoint Policy Management: Enforce assessment and remediation of endpoints during the Internet authentication sequence, prior to allowing VPN access. A network connection is only granted after checking for policy compliance and taking corrective action to update the endpoint to a trusted state.

Establish Universal Policy Enforcement: Ensure users to go through policy checkpoints before granting network access by forcing the use of iPassConnect for Internet access, restricting VPN use through DeviceID and requiring assessment and remediation through Endpoint Policy Management. The combination of these steps provides the deepest level of policy enforcement.

In these ways, DeviceID helps you support the enterprise goal of protecting the corporate network by ensuring the integrity of the endpoint devices attaching to it. Not only does DeviceID help you enact policies that harden endpoint security, all this is accomplished without impeding user productivity or making management more difficult for IT staff.

DEVICE VISIBILITY AND TRANSPARENT ENFORCEMENT LOWER TCO

With DeviceID, you can add strong two-factor authentication that enables transparent VPN policy enforcement without impeding user productivity. For DeviceID users, there's no hardware or token to break, lose or hassle with and— unlike digital

certificates — nothing is left on the PC for hackers to copy and export. For IT, a robust Web portal makes DeviceID simple to administrate and provides powerful real-time reporting.

Easy to Implement and Use: Make deployment hassle-free for IT staff and end users alike through transparent registration and activation. Upload users from existing databases; silently distribute, install and activate the DeviceID software.

Transparent Authentication: Provide device-level authentication through the same authorization process with which users are already familiar. Since DeviceID doesn't alter the end-user experience, there's no user interaction, learning curve or training required.

Real-time Reporting: Generate and filter reports by user, machine, transaction type and status for granular control over who accesses the network and from which devices. Reports are pulled directly from the DeviceID database, ensuring a full audit trail of all network activity.

CONFIDENCE, PLAIN AND SIMPLE

Through DeviceID, iPass continues to deliver on its promise of trusted connections; no compromises. Seamless integration with iPassConnect and Endpoint Policy Management enables DeviceID to ensure that only trust-worthy devices are allowed VPN access to the corporate network from home, around town and around the world. Learn more about the role DeviceID plays in providing a connectivity solution that truly enforces security policies over any Internet connection while keeping mobile workers productive. Visit www.ipass.com or talk to your iPass account manager today. ■

SUPPORTED VPNS:

Nortel VPN Client
Cisco VPN Client
Microsoft PPTP VPN Client

SUPPORTED AAA:

Active Directory 2003
Cisco ACS 2.8

SUPPORTED CLIENT PLATFORMS:

Microsoft Windows XP
Microsoft Windows 2000

SUPPORTED IPASS SOFTWARE:

iPassConnect 3.35 and above
Endpoint Policy Management—Online 3.0 and above
Endpoint Policy Management—Enterprise 7.0 and above

REQUIRED SERVER SOFTWARE:

Microsoft Windows 2003, Microsoft Windows 2000 with Service Pack 4,
Microsoft Windows 2000 Advanced Server with Service Pack 3
Oracle 9i
Microsoft IIS required for admin portal
Internet Explorer 6.0 and above required for admin portal

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065

+1 650-232-4100
+1 650-232-4111 fx

www.ipass.com

