Honeywell Integrated Security

Honeywell

Identity-based Integration for Stronger Security

Identity-based Integration for Stronger Security

SmartPlus™ Imprivata® Connector

Like you, thousands of companies routinely control building access using Pro-Watch®, Honeywell's advanced access control system. In parallel, you also manage IT network access using enterprise network authentication infrastructure. Today, the physical and the logical live in separate technology silos. But what if you could enable seamless communication between the two systems to effect a stronger, and more compliant, overall security posture?

Introducing SmartPlus Imprivata Connector – your solution for stronger enterprise security.

The SmartPlus Imprivata Connector uses OneSign™ Physical/Logical to enable Pro-Watch to provide a single point of authentication management. It effectively closes security gaps that exist when physical access control and IT network authentication systems live in self-contained silos.

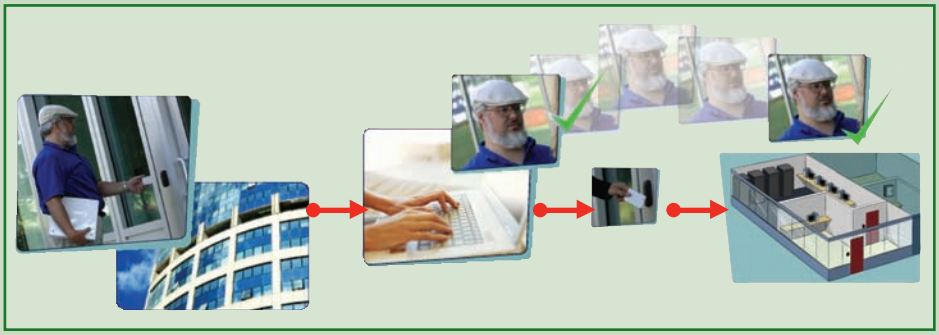
Using a single Web-based interface, OneSign Physical/Logical enables the mapping of identities contained within Pro-Watch and corporate IT directories. The SmartPlus Imprivata Connector allows network access and badging privileges based on an employee's status, role within the organization, and/or physical location.

- **Leverage your proven Pro-Watch system to improve IT security and increase the value of your Pro-Watch system investment.**
- **Audit who, what, when, and from where – whether from door, desktop, or remotely, to better demonstrate compliance and leverage both systems from one location.**
- **Strengthen your overall security to close security gaps between disparate security systems.**
- **Quickly deploy a converged security system without modifying Pro-Watch or IT infrastructure.**

The SmartPlus Imprivata Connector helps Pro-Watch® work together seamlessly to address the following security scenarios:

Tie Network Access to Physical Location

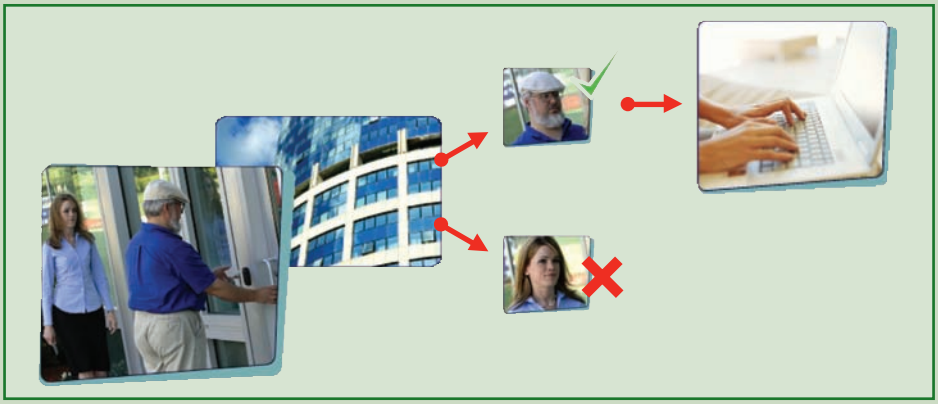
Gain greater security control by tying network access to badging into the building – or a zone or room within the building – in order to ensure only valid employees gain access. In addition, if a remote VPN access request comes in from a user ID that is already authenticated within the building and to the local network, OneSign will deny remote access, mitigating rogue, remote VPN access attempts.



Tie network access to badging into the building.

Enforce Your Anti-Tailgating Policy

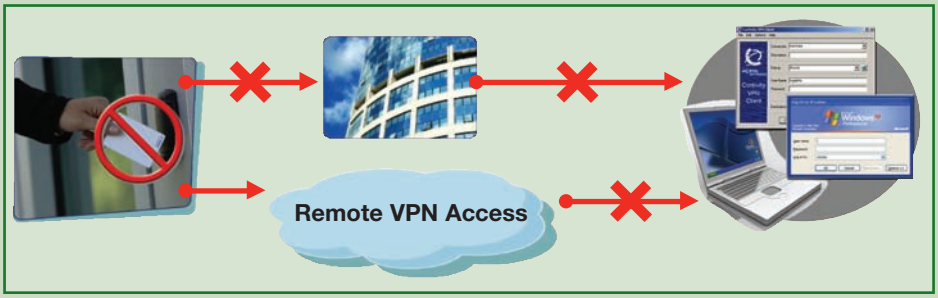
Anti-tailgating or piggybacking policies are difficult to enforce without deployment of expensive and burdensome turnstile ingress/egress systems. The combined power of Pro-Watch and OneSign works to enforce anti-tailgating policy by tying a user's building badge events with network access. If a user does not badge into your building, he doesn't get access to the network.



Tie a user's building badge events with network access.

Instant User Lock-Out

Revoking a user from Pro-Watch instantly locks the user from network access, both local and remote VPN. Instant user lock-out effectively closes security gaps that exist between the days or weeks—or in some cases, never—of deprovisioning non-active identities from local and remote IT directories.



Revoke a user from Pro-Watch instantly.

Consolidated Monitoring and Reporting – Compile Forensic Timelines

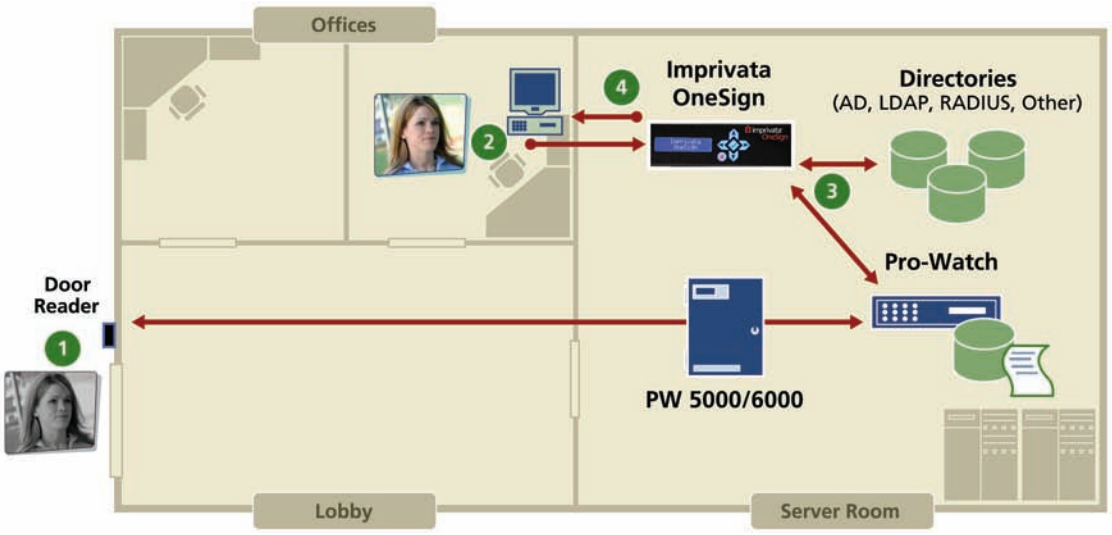
Quickly and easily consolidate user access reports for building, zone, network, and remote access. Your ability to monitor and report who is accessing what, when, and from where is a critical component for demonstrating compliance, both for the purpose of government regulations and corporate security forensic investigations. Converged reporting has never been easier!

System Ready; Non-disruptive

OneSign interoperates with your existing Pro-Watch and IT network infrastructure. OneSign's appliance-based packaging enables seamless communication between Pro-Watch and IT security environments for non-disruptive, identity-based convergence. No changes to your Pro-Watch or IT directories are required, no Pro-Watch or IT system modification is required. You can now achieve even greater protection of your enterprise assets while maximizing the value of current security infrastructure.

SmartPlus Imprivata Connector:

Pro-Watch and OneSign Working Together



1. User taps Door Reader with access card; Pro-Watch verifies user and unlocks door
2. User attempts login to network, initiating authentication call to OneSign
3. OneSign verifies with Pro-Watch that user is active and badged into the building; OneSign verifies user's network privileges with IT Directories
4. OneSign authenticates user to the network

Benefits of Pro-Watch and OneSign Integration …

Benefits for IT Security

- Close security gaps with Instant User Lock-Out
- Two trusted identity sources for authentication to the network
- Increased security with network authentication based on location
- Comprehensive and easy compliance reporting

Benefits for Physical Security

- Enforce anti-tailgating policy
- Improve operational efficiency and reduce insurance liability
- Maximize value from Honeywell Pro-Watch system investment
- Comprehensive and easy compliance reporting

… and for the user, no changes to their existing workflow.

Radically Easy

SmartPlus Imprivata Connector is an appliance-based solution. No scripting or custom code is required. It's Honeywell Pro-Watch ready; nothing extra to buy, install or modify.

Simply Smart

The SmartPlus Imprivata Connector ensures your company resources are being used only by authorized employees and creates a finer grain of authentication to sensitive network resources. Policy can be applied to determine that certain groups of individuals such as research scientists can only log onto computers within a secured lab after they have first badged into the lab.

- Enables use of one policy for allowing or denying network access based on a user's journal entries for physical location and/or employee badge status.
- Eliminates "tailgating/piggybacking" behavior.
- Integrates and centralizes monitoring and reporting.
- Controls who is accessing what, when, and from where.
- Compiles forensic timelines from building entry to desktop and application logon.

Uniquely Affordable

With SmartPlus Imprivata Connector, you can extract greater value from your existing keycard and door readers by building a more secure network environment.

- Interoperable with existing network authentication infrastructure, delivering a solution that works together now.
- Maximizes existing security investments.
- Building access card independent; works with all current and future card types.
- Reduces insurance liability and improves operational efficiency.
- The SmartPlus Imprivata Connector works to quickly and effectively solve password management, security and user access issues to all enterprise applications – legacy, client/server, JAVA, and Web – without requiring any custom scripting, changes to existing directories, or inconvenient end user workflow changes.

For more information:
www.honeywellintegrated.com

Honeywell Security
Honeywell Integrated Security
2700 Blankenbaker Pkwy., Suite 150
Louisville, KY 40299
800-323-4576
www.honeywell.com

L/SMRTPLSB/D
October 2007

Honeywell