

C•CURE® 800/8000 Physical/Logical Access Control Solution

utilizing Imprivata® OneSign™
identity-based convergence system



Features That Make a Difference:

- Links IT Network access with C•CURE® 800/8000 access control events
- Provides single-point authentication management using password, password and card, or password and biometric
- Helps organizations comply with regulations such as Sarbanes-Oxley, HIPAA, etc.
- Browser-based graphical user interface makes it easy to connect from any PC with an Internet connection
- Strengthens anti-tailgating policies
- Instant user lock-out feature closes security gaps
- Reduces security risk when non-active employees are instantly revoked from local and remote IT directories
- Appliance-based package easily plugs into your network

The C•CURE 800/8000 Physical/Logical Access Control Solution utilizes Imprivata OneSign identity-based convergence system to share information between a company's C•CURE 800/8000 security management system and the company's network.

OneSign allows quick and easy emergence of user activity from the C•CURE 800/8000 system to detail and monitor who is accessing what, when, and from where in order to grant access to the network. This is crucial for complying with regulations such as Sarbanes-Oxley, HSPD-12, HIPAA, and corporate security investigations.

This solution provides enhanced security during authentication by requiring a user to present a password, password and card, or password and biometric when accessing a building and signing on to a networked system.

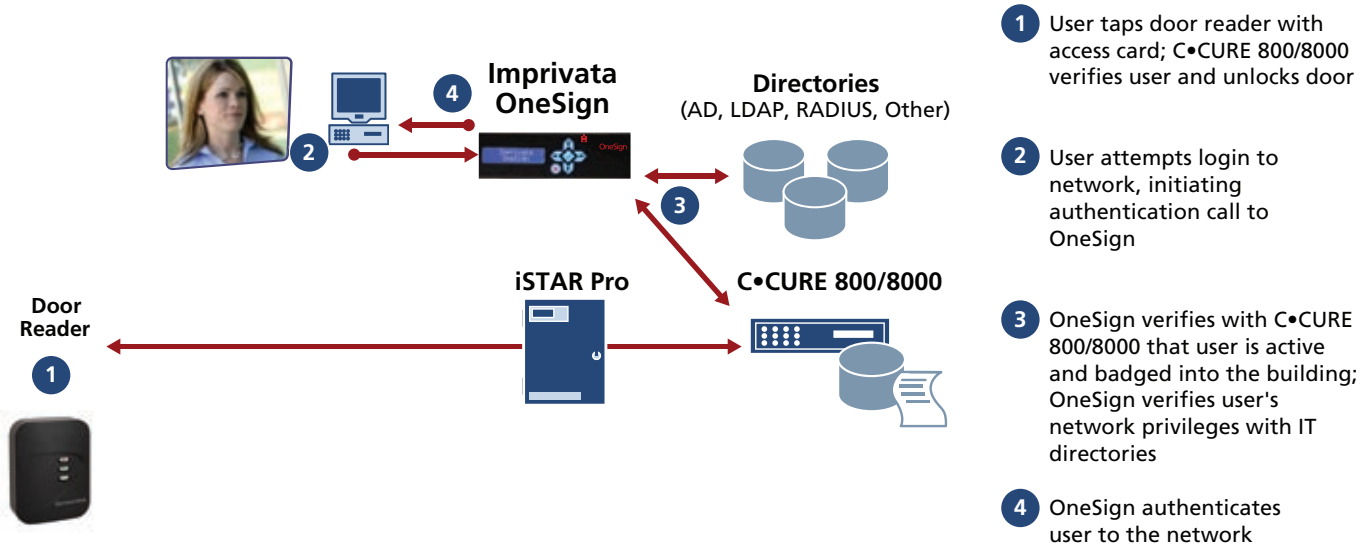
By linking a user's physical access badge activity with network access, this integrated solution strengthens anti-tailgating policies. For example, if an individual enters a building/zone behind another individual without presenting his/her card

s/he can be rejected from accessing the network. This allows corporations to reduce costs by eliminating burdensome turnstile ingress/egress systems.

The OneSign application utilizes a browser-based graphical user interface that lets you easily make all system configurations from any computer with an Internet connection.

The C•CURE 800/8000 Physical/Logical Access Control Solution effectively closes security gaps with an instant user lock-out feature. This feature instantly locks the user from the network once revoked from the C•CURE system, eliminating the risks associated with the time gap that can exist between an employee's termination date and removal from the network.

The OneSign appliance-based package easily plugs into your network and no configuration changes or modifications to your C•CURE 800/8000 system or network are required.



- 1 User taps door reader with access card; C•CURE 800/8000 verifies user and unlocks door
- 2 User attempts login to network, initiating authentication call to OneSign
- 3 OneSign verifies with C•CURE 800/8000 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

Application Environments Supported

- ALL browser-based applications running in Internet Explorer 5.5 SP2 or higher on supported Windows OS.
- ALL Mainframe, AS/400, UNIX, other legacy applications accessed via Terminal Emulators (TEs).
 - TEs that support a HLLAPI interface on supported Windows OS
 - Non-HLLAPI TEs
 - Web-to-Host clients
 - Console-based applications launched from a Windows command line
- ALL Win32 client-server or client applications on supported Windows OS.
 - Windows applications
 - Java applications using SUN, Oracle or IBM JVM
 - Custom and legacy applications, running on a supported Windows OS

Administration Console Requirements

- Internet Explorer 6.0 SP1 or higher running on Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003. USB is required for finger biometrics and proximity cards.

Client Systems Supported

- Internet Explorer 5.5 SP2 or higher running on Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003. USB is required for finger biometrics and proximity cards.

Directories Supported

- Microsoft Active Directory 2000 / 2003 Server, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID) 10g, Novell Netware 5.1 running NDS 8.0 or later, Novell eDirectory 8.0 (8.1 required for SSPW Management), IBM Tivoli LDAP.

Appliance

- Pair of ready-to-use redundant 1U rack mountable servers. Failover is included. Operating system is SUSE® LINUX Enterprise 9 from Novell.

Internationalization

- The Imprivata OneSign secure database and internal data structures are fully Unicode multi-byte enabled. Usernames and passwords can be supported in single or multi-byte character sets for Enterprise Single Sign-On (ESSO) and PW management for all users.
- The OneSign administrators' browser-based UI remains English-only for system configuration and management.
- All OneSign Agent (user-facing) desktop dialogs and messages are localized for English, French, German, Spanish, and Italian.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative. Certain product names mentioned herein may be trade names and/or registered trademarks of other companies.

©2007 Sensormatic Electronics Corporation. All rights reserved. SH0102-DS-200710-R01-LT-EN