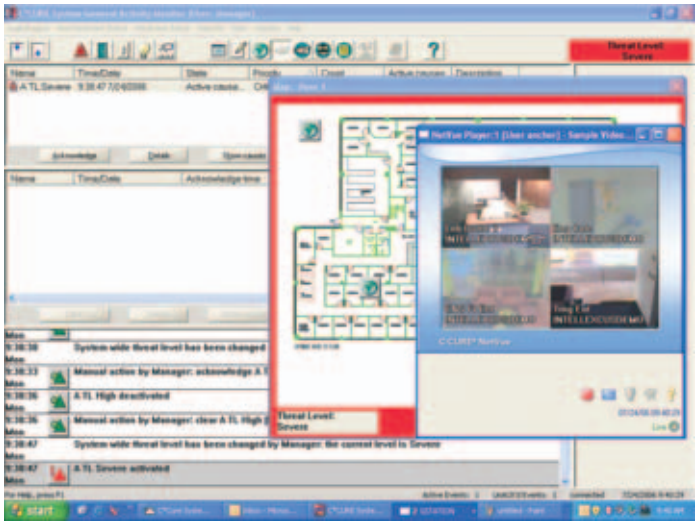
SOFTWARE HOUSE®

DATA SHEET

C•CURE® 800/8000

Security Management Solution



Features that make a difference:

- Advanced event and alarm monitoring solution provides flexible and powerful control
- Easily integrate with digital video management systems and other business-critical applications
- Significantly enhance security with intrusion zones and keypad commands
- Easily create cardholder unique identifiers (CHUIDs) with extended card number support
- Assign up to 5 cards per cardholder, including a PIN only credential
- Monitor multiple locations from a single guard station
- Extraordinary threat level support allows you to change the operation of the system based on current events
- Dynamic clearance filters ensure personnel clearance numbers match the clearance number of the protected area
- Intuitive .NET badging solution provides high performance, cost-effective identification management system
- Powerful database partitioning gives maximum security to buildings with multiple tenants

Complete Integration with Unlimited Applications

C•CURE 800/8000 is a scalable security management solution encompassing complete access control and advanced event monitoring. The system integrates with critical business applications including CCTV and digital video such as the American Dynamics Intellex® digital video management system, visitor management, ERP, HR/time and attendance, and third party devices such as fire alarms, intercoms, burglar and other alarms.

Easy to Network

C•CURE 800/8000 client workstations and iSTAR® and iSTAR eX controllers can be placed directly on an existing network and across a wide area network (WAN). iSTAR controllers support dual network connectivity and Dynamic Host Configuration Protocol (DHCP), easing connectivity to most existing networks.

C•CURE 800/8000's open architecture design ensures universal support and enormous system flexibility by allowing the system to interact with industry standard databases, video recorders and cameras, and network devices.

Ideal for government and enterprise customers

Whether it's specifically complying with FIPS regulations, or ensuring that safety precautions are augmented when critical security events occur, C•CURE 800/8000 is the system of choice for meeting today's most stringent security regulations and demanding administrative operations. In addition, C•CURE 800/8000 supports the iSTAR eX Ethernet-ready controller to provide an encrypted security solution for government applications or for any enterprise looking for the highest security available in the industry.

Accountability and Auditing

A comprehensive audit trail is critical for pharmaceuticals and healthcare facilities that must comply with process regulations. C•CURE 800/8000's field-level audit trail enhances the control you have of data and system integrity by tracking changes made to all relevant security objects, including configuration and clearance data.

Unlimited Scalability

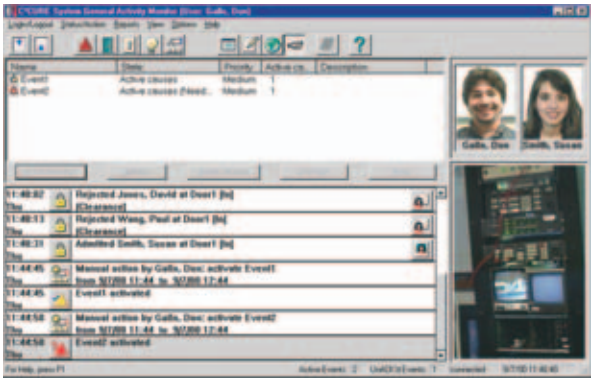
C•CURE 800/8000 is completely scalable and lets you easily add functionality and increase capacity as your security needs grow. Using .MSI, Microsoft's standard installer technology, C•CURE 800/8000 lets you easily install, upgrade, and repair remote C•CURE 800/8000 workstations quickly and easily without visiting every site.

tyco / Fire & Security

take a closer look

Advanced event and alarm monitoring station provides flexible and powerful control

The C•CURE 800/8000 monitoring station displays cardholder images based on granted/rejected access or events. For added convenience, you can name, prioritize and sort alarms as they occur right at the C•CURE 800/8000 monitoring station. For example, you can choose to name your alarm categories, such as "1-Life Safety, 2-SCI, 3-DoD, and 4-General" in place of the default Critical, High, Medium and Low, which allows you to customize the interface based on your security parameters. You can also easily sort alarms by priority and/or date and select from up to eight unique defined priority labels and more than 16 million colors for coding priorities.



For an easy way to manage critical alarms, a powerful dual acknowledgment screen lets you retain a record of events after all of the active causes behind them have been resolved. It's an extremely effective way to manage new alarms as they arise without losing track of those still under investigation.

Monitor multiple locations from a single guard station

With the C•CURE 800/8000 central monitoring option, users can monitor multiple widely dispersed locations from a single monitoring station, providing total enterprise security management.

Powerful database partitioning gives maximum security to buildings with multiple tenants

C•CURE 800/8000 allows groups to share a single database while, at the same time, partitioning to maintain individual groups' security. Partitioning supports multiple tenant locations at one site or it can support a single organization occupying multiple buildings, ensuring that security officials have access only to information that is pertinent to their facility.

Integration with digital video management systems and other business-critical applications ensures total control

Using the powerful application programming interface (API), C•CURE 800/8000 provides seamless integration with select digital video management systems (DVMS), including American Dynamics Intellex, via its NetVue application. This integration allows you to tie an event generated on C•CURE 800/8000 to live video. With enhanced alarm management, NetVue can automatically activate C•CURE 800/8000 events based on motion detection alarms received from a DVMS. Refer to the C•CURE NetVue datasheet on www.swhouse.com for more detailed information.

For integration with many other devices, such as fire panels and intrusion detection systems, the bi-directional serial interface can be used to receive and interpret messages sent to C•CURE 800/8000. These messages can trigger events and generate a journal entry on the monitoring station. The interface can communicate with the C•CURE 800/8000 via an RS-232 serial port or remotely through TCP/IP via a qualified terminal server.

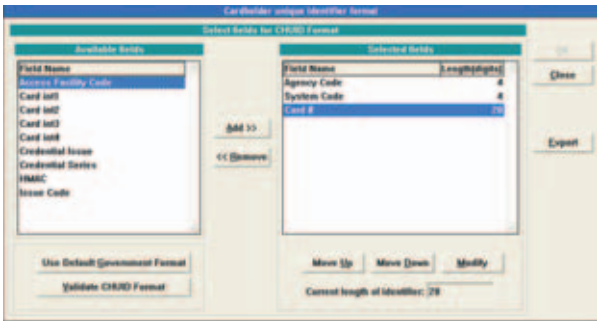
features

Significantly enhance security with intrusion zones and keypad commands

An intrusion zone is a group of doors and inputs that defines a physical area that is monitored for alarms. Grouping inputs and doors into intrusion zones allows easy collective arming and disarming of alarm monitoring points (inputs) as well as locking and unlocking groups of doors while displaying their current mode and status. Leveraging the intrusion zone feature, you can use keypad commands to remotely activate camera, door and other events from an RM reader keypad connected to an iSTAR controller. Keypad commands provide a powerful way to trigger a duress call, sound an alarm, lock and unlock doors, and more, directly from an RM reader keypad. Keypad commands can be configured to require a card presentation and/or a PIN to validate the command.

Easily create CHUIDs with extended card number support

C•CURE 800/8000 supports extended card numbers[1] which allows users in government applications to comply with certain federal guidelines (such as FIPS 201) that require a multi-field CHUID. In addition, iSTAR controllers support card numbers of up to 256 bits, eliminating the need for multiple facility codes, site codes, or offset in order to avoid card duplication. Longer card numbers offer greater protection against card duplication and are especially valuable to customers who require card numbers that exceed 10 digits.



Assign up to 5 cards per cardholder, including a PIN only credential

C•CURE 800/8000 lets you assign up to 5 cards per cardholder record, rather than having to create a separate record for each card. Using this powerful feature, you can assign a PIN as one of the cards, providing a flexible and secure solution and greatly simplifying the management and maintenance of personnel records.

For additional flexibility, you can use iSTAR controllers to support up to 128 card formats system-wide and 10 card formats per reader. This expanded ability to use multiple card types (such as 26-bit, 37-bit, or Corporate 1000) at a single reader frees you from having to consolidate or re-issue new cards.

Controlling areas and managing occupancy levels helps you maintain safety regulations

Once someone is granted access to the building the real work begins to ensure that confidential areas are kept protected, occupancy levels are maintained for safety, and the general well being of employees and visitors is ensured. C•CURE 800/8000 lets you easily configure all of the areas in your building and across multiple buildings and identify inbound and outbound readers to enforce anti-passback. This allows you to prevent someone from passing his/her access card back to another person for unauthorized entry, using either a timed or event-driven configuration. Area Lockout operates in much the same way, but takes it a step further by actually locking a cardholder out of an area based on a decrementing timer specification.

Managing occupancy levels is another powerful capability that lets you define how many people and/or what type of person is allowed in a room. This type of control is essential for extremely classified areas, such as Secured Compartmentalized Information Facilities (SCIFs) which exist most often in the government-related marketplace. In these sensitive instances, you can configure C•CURE 800/8000 to require a supervisor to be present before allowing an employee to access the area. This type of restriction can also apply to visitors who may require an escort as they pass through restricted doors.

[1] Only with iSTAR controllers

Threat level support allows you to change the operation of the system based on current events

C•CURE 800/8000 provides a solution for government agencies needing to comply with the Department of Homeland Security requirements by allowing them to change the operation of the security system based on a threat level. For example, if the national threat level (defined as “Low”, “Guarded”, “Elevated”, “High”, and “Severe”) is raised, the administrator can react by changing the threat levels in the C·CURE 800/8000 system, which may then be configured to react in the following user-defined ways:

- **Cardholders may be required to present a higher level of credential to gain access to a door.**
  During a “High” threat level, cardholders may be required to use a Personal Identification Number (PIN) in addition to presenting their proximity card. In some instances, an elevated threat level might also require that personnel have approved escorts in order to gain access.

- **Operators or guards may need to validate their manual actions with an approved response.**
  Under normal circumstances, guards may be able to freely execute manual actions, such as temporarily unlocking a door or gracing a card from the guard station. But, in higher threat levels, these types of manual actions would be challenged by the system, requiring an approved response from the operator performing the action. For example, the operator will be required to enter in a secret code, or input a journal entry before the manual action will be approved. In addition, operators may be required to acknowledge each and every alarm on the guard station, ensuring proper attention is being paid to potential risks.

- **Events may be automatically activated**
  When the system is set at certain threat levels, specific events can be activated throughout the entire facility, on a wide range of readers, or on specific controllers. For example, if the threat level is set to “Critical” on the C•CURE 800/8000, this can automatically deploy road bollards in designated security-critical roadways. Or, clearance filters, a powerful, new feature that forces the cardholders’ credentials to exactly match the credential at an affected reader, can be enforced based on specific security or threat levels.

- **Display current threat level color on maps and monitoring station for consistent reminder of status**
  Ensuring that the current threat level is kept top of mind by the operator or guard, the monitoring station and maps both highlight the color that is associated with the threat level.

- **An escort may be required**
  During elevated threat levels, the system may require that all visitors must be escorted by authorized personnel in order to gain access to protected areas.

	MODEL 1	MODEL 5	MODEL 10	MODEL 20	MODEL 30	MODEL 40	8000 Enterprise Server	8000Plus Enterprise Server
Number of Online Readers*	32	64	128	256	512	1000	2500	*
Number of Online Inputs	128	256	512	1024	2500	5000	10000	*
Number of Online Outputs	128	256	512	1024	2500	5000	10000	*
Number of Addressable Controllers	No limit	No limit	No limit	No limit	No limit	No limit	No limit	No limit
Number of Cardholders*	10K	40K	40K	250K	250K	250K	500K	500K
Number of Assets	N/A	40K	40K	250K	250K	250K	500K	500K
Number of Simultaneous Client PCs Included with Server	2	3	4	8	16	64	128	128
Number of Client PCs Definable on Server	999	999	999	999	999	999	999	999
Sentinel Required	YES	YES	YES	YES	YES	YES	YES	YES

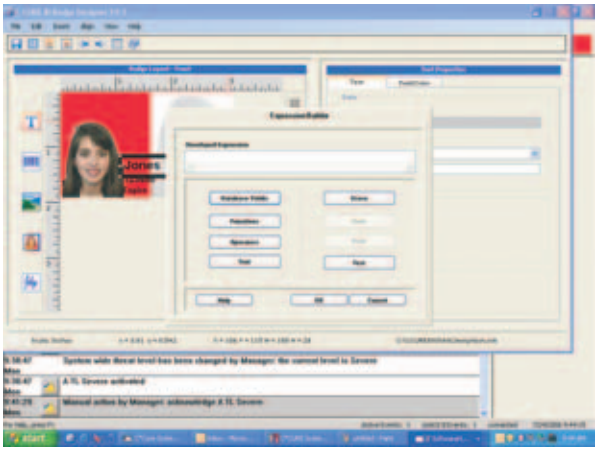
* C•CURE 800/8000 is designed for unlimited expansion. The often stated 3,000 reader and 32,000 input/output handling are tested limits only and do not represent expansion restrictions. System performance will vary depending upon specific hardware configuration including number of communication lines/ports, download/upload frequency, etc.

Dynamic clearance filters ensure personnel credentials match the clearance number of the protected area

C•CURE 800/8000 includes a feature that allows you to assign a clearance filter number to personnel which must match the clearance filter number of the reader in a protected area. For example, an operating room may be accessible to all hospital personnel during non-surgery times. At these times, the reader that secures the room has a clearance number of “1” and each person with a clearance filter number “1” can gain access. During operations, however, the clearance filter on the reader automaticall changes to a “3”, which means only those personnel who have a clearance filter of “3” will bepermitted access. This is done without changing the underlying clearance available to the area.

Intuitive .NET badging solution provides high performance, cost effective identification management system

Access control cards are essential for security, but can also be a nice way to communicate your company’s message to employees and the public. The C•CURE 800/8000 badging solution utilizes Microsoft’s .NET guidelines for the graphical user interface and offers superior control of color and graphics, providing the ability to create professional, sophisticated badges.



Specialized display needs for badge layouts are common and the Expression Builder allows you to easily meet these needs by simply picking fields from a list that builds sophisticated expressions, without ever having to understand the complexity of expressions. For example, if you want to ensure that an employee's middle initial is printed wherever appropriate, an expression allows the customer to easily do this without adding blank lines where cardholders may not have a middle initial.

In many instances, a company can have hundreds, even thousands, of badges in the system. C•CURE 800/8000 also makes it extremely easy to manage your badges by allowing you to query on a common field and then print those found by that query in one batch. Refer to the C•CURE ID datasheet on www.swhouse.com for more detailed information.

Managing access control using a graphical interface

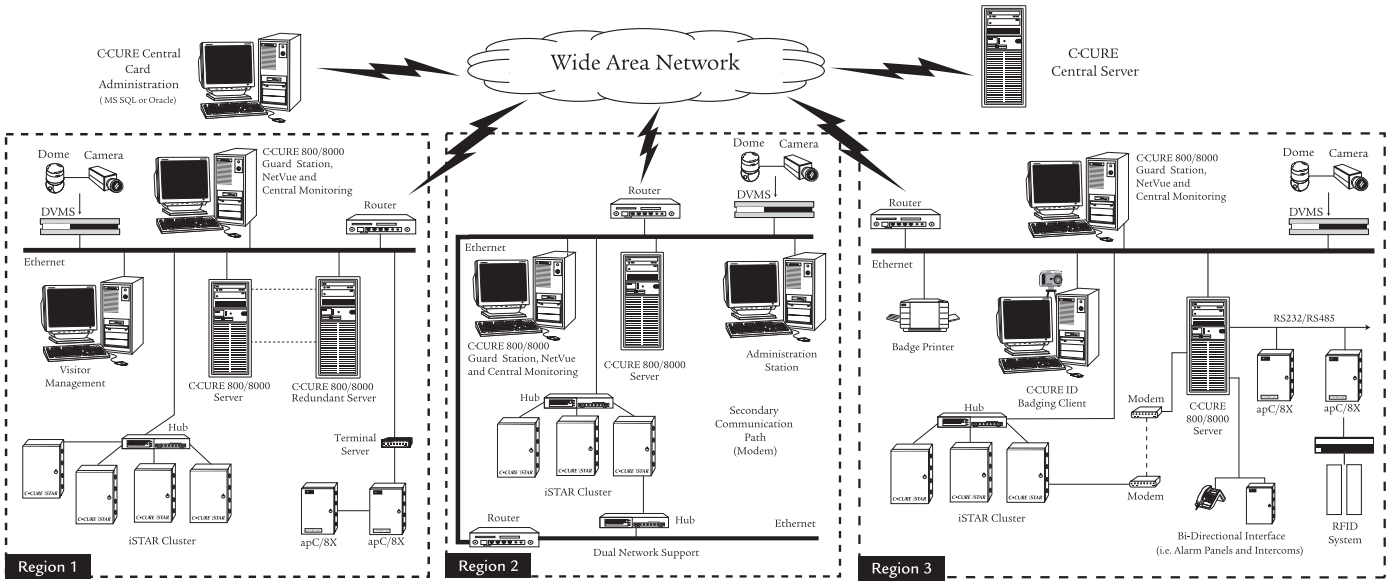
C•CURE 800/8000’s map interface allows you take any CAD drawing or Visio file, save it as .bmp and then populate your map with icons that reflect security objects, such as doors, inputs, outputs, cameras, events, video tours and views. You can also nest maps within maps to provide an easy interface that lets you travel graphically around your facility and manage events directly from the map.

At the monitoring station, you’ll immediately see the benefits of the mapping feature when a critical event such as “Door Forced Open” occurs. This event can cause a live video window to automatically pop-up on the map, giving you the exact location and corresponding video footage. Here, the nested maps come in very handy to help you drill down to graphically navigate through the facility looking for the person who may have caused the Door Forced Open event. Using the dynamic icons and the powerful NetVue interface, you can even launch a video tour of the affected area to immediately investigate.

For more sophisticated management of a building layout, C•CURE 800/8000 has solid integration with a third party graphical interface called AEGIS which lets you account for walls that have beeen knocked down, doors that may have been moved, expansion projects and more.

SOFTWARE HOUSE®

SPECIFICATIONS



C•CURE 800/8000 Server Recommended Minimum Requirements

Processor

- Model Number 1 through 10 . . . . . .1.5 GHz Intel Pentium III or higher
- Model Number 20 through 40 . . . . . .1.8 GHz Intel Pentium III or higher
- Model 8000 and 8000 Plus . . . . . .2.4 GHz Intel Pentium IV or higher
- Free Hard Disk Space . . . . . .3.0 GB

Memory

- Model Number 1 through 40 . . . . . .1 GB RAM
- Model 8000 and 8000 Plus . . . . . .2 GB RAM

Network Card . . . . . .10/100 Base-T
DVD Drive 2X
Monitor/Video Adapter board . . . . . .17" SVGA (1024 x 768)
Operating System . . . . . Windows® Server 2003, Windows XP Professional (Service Pack 2)
Mouse . . . . . .PS/2 bus type
Ports . . . . . .2 serial, 1 parallel, USB
(with C•CURE 800/8000 v8.x a USB port is required)
Backup . . . . . .Tape or CDRW
Modem . . . . . .56.7 Kbps
Sentinel . . . . . .Supplied by Software House
Digiboard . . . . . .8 port (Models 20/30/40

C•CURE 800/8000 Client Recommended Minimum Requirements

Processor . . . . . .1.5 GHz Intel Pentium or higher
Free Hard Disk Space . . . . . .2.0 GB
Memory . . . . . .512 MB RAM
Network Card . . . . . .10 Base-T
CD-ROM Drive 10X
Monitor/Video Adapter board . . . . . .17" SVGA (1024 x 768), 64 MB RAM
Operating Systems . . . . . .Windows XP Professional (Service Pack 2)
Mouse . . . . . .PS/2 bus type

Note: It is recommended that customers use the most current firmware release for each controller.

www.swhouse.com

Microsoft GOLD CERTIFIED Partner

ISV/Software Solutions
Networking Infrastructure Solutions

tyco / Fire & Security