SOFTWARE HOUSE

C•CURE Solutions
SALTO Offline Locks

Features That Make a Difference:

- Seamless integration with C•CURE 9000 security and event management system

- Offline, wireless and wireless-ready locks supported

- High level interface between C•CURE 9000 and offline lock system using SHIP (SALTO Host Interface Protocol)

- SALTO online readers to update cards for offline reader access

- Offline transactions shared via cards are synchronized with C•CURE 9000 server

- Suitable for storage areas, office spaces and other areas where real-time security monitoring is not a priority

- Flexible design that can be fitted to almost any type of door

- Ideal to replace a key management system

The C•CURE 9000 integration with SALTO offline locks allows communication with the SALTO server and control of cardholder access permissions to offline locks, directly from the C•CURE 9000 system. This seamless interface supports bi-directional communication with the SALTO system using SHIP (Salto Host Interface Protocol). The SALTO offline lock solution offers flexibility within any project where the cost of a fully wired door is not justified. SALTO offline locks can be installed on almost any type of door ranging from narrow profile, aluminum doors, heavy duty doors, panic bars, glass doors and many more. With the SALTO offline lock solution no cabling is required to the actual lock installation. If required, door inputs can be wired separately to Software House online devices for real-time monitoring. Doors fitted with SALTO offline lock technology are integrated and managed within the existing C•CURE 9000 system.

SALTO Online Reader Control Points

Offline locks can be accessed by a card holder only after appropriate access permissions are written to the card by swiping a card at a control point reader. This will update and activate access to offline locks. The offline lock access permissions are managed on the central C•CURE 9000 system. By default,

access to offline locks will expire after one day, unless a card is updated with a fresh update point transaction.
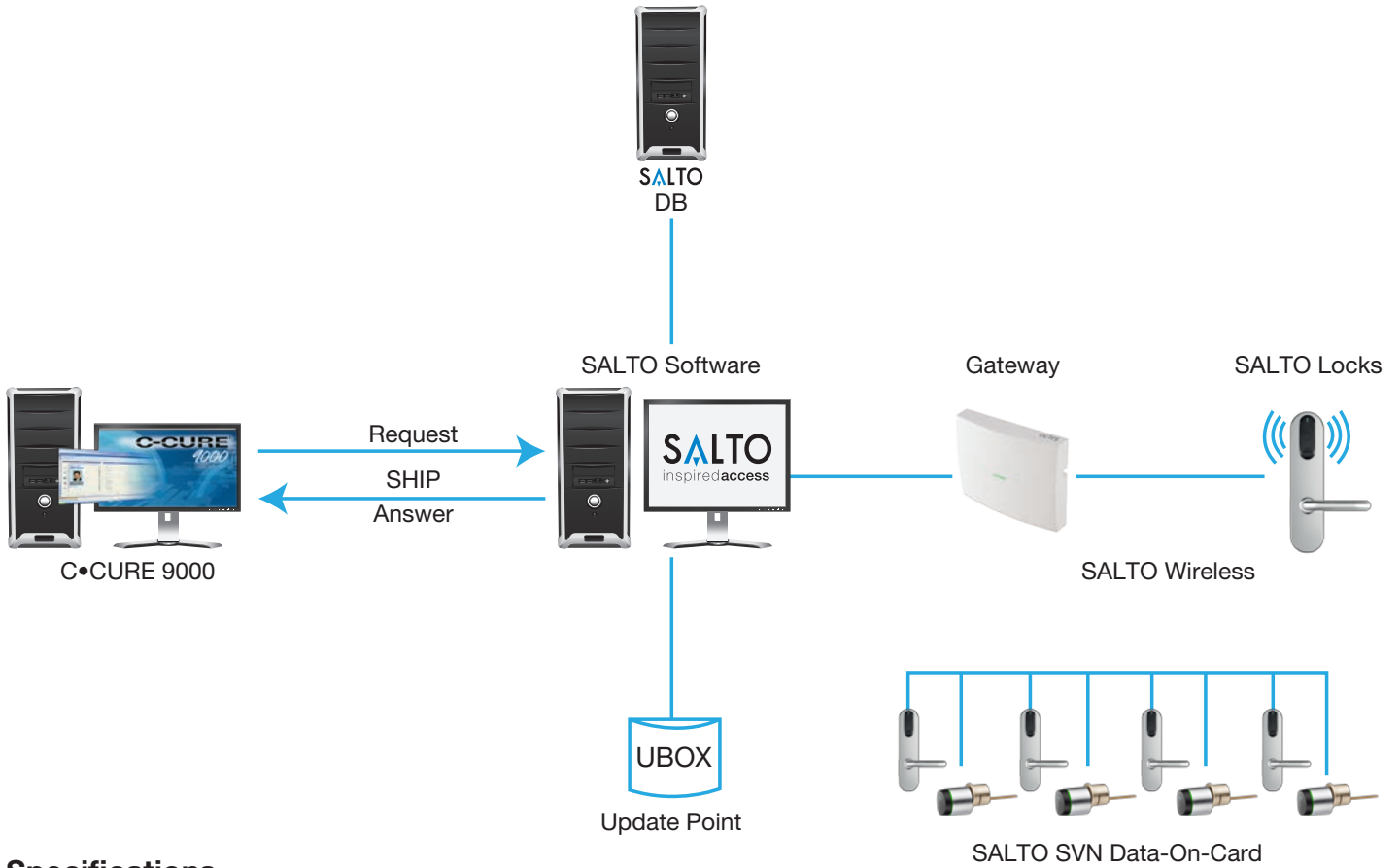
SHIP Interface

C•CURE 9000 support for SALTO offline locks utilizes a high level interface to SHIP (SALTO Host Interface Protocol). C•CURE 9000 and the SALTO offline lock solution exchange cardholder data via SHIP communications over an Ethernet network. SALTO online readers (control points) are used to update a card with access permissions for offline lock use. In addition, cardholder offline door transactions are also reported back to the SALTO server. C•CURE 9000 will poll the SALTO server frequently to retrieve offline transactions for reporting purposes.

Nested Offline Lock Access Control

In the case when highly secure Software House readers and real-time monitoring are not required, doors can be fitted with SALTO offline lock technology, creating a fully integrated and managed lock solution within C•CURE 9000. Offline locks can be placed into a controlled nested area, for example within a zone of online Software House readers for added security.

SALTO
inspired**access**

C•CURE 9000/SALTO System Diagram

SALTO DB

SALTO Software   Gateway   SALTO Locks

Request

SHIP

Answer

C•CURE 9000

SALTO Wireless

UBOX

Update Point

SALTO SVN Data-On-Card

Specifications

C•CURE 9000 Software Requirements

C•CURE 9000. . . . . Version 2.40 or greater (check Software House Connected Compatibility Matrix for current support information)

C•CURE 9000 Enterprise . . Not supported at this time

SALTO Server Minimum Requirements

Component	Requirement
RAM	4 GB
Processor	1 GHz or higher
Display	1024 x 768 high-color, 32-bit display
Hard Disk Space	10 GB (recommended required space to operate a database in a large organization)
Operating System	Windows Vista, Windows 7, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2008 R2 and Windows Server 2012 (32-bit and 64-bit)
MS SQL Server	Versions 2005, 2008, 2008 R2, 2012, 2014 and LocalDB (all editions, including MS-SQL Express). If the SALTO database was originally created with MS SQL Server 2000 and higher migrated to a higher version, you must ensure that the database is in compatibility level 90 (version 2005) or higher.
Machine Name Resolver	Domain Name System (DNS)
Domain Environment	A shared network is required and the domain or work group must be set up by the organization's IT administrator. This is strongly recommended as it simplifies security and permission issues.

Maximum SALTO locksets
per SALTO Server...................64,000

SALTO ProAccess SPACE Minimum Requirements

Component	Requirement
RAM	1 GB
Processor	1.6 GHz or higher (x 86 or x 64)
Operating System	Windows Vista (32-bit and 64-bit) or higher
.NET Framework	Version 4.0.2 (included with the installation file)
Plugin	Silverlight 5
Web Browser	Microsoft Internet Explorer (9 or higher) - Due to its compatibility with Silverlight, Microsoft Internet Explorer is the only browser recommended for use with ProAccess SPACE.

SALTO Card Specifications

Card Types Supported . . . . DESfire, DESfireEV1, MIFARE, MIFARE Plus, Legic Prime, Legic Advant, HID iCLASS

Minimum Card Memory
Required for Audit on Card. . 416 bytes (9 sectors on a MIFARE Classic card, allows 14 events per card)

Maximum Number of
History Messages Stored
on Card . . . . 50 messages (MIFARE 1K), 380 (MIFARE 4K)

Maximum Number of Cards
per SALTO Server . . . . 4,000,000 (64,000 max can be subject to blacklist)

SALTO Justin Mobile or
Justin mSVN Mobile
Credential Support . . . . No

Specifications for Wireless Option

Software House also offers SALTO wireless-ready lock models for customers who may want to have wireless in the future but are not ready to invest in a full wireless solution.

Wireless Technology . . . . . . IEEE 802.15.4, 2.4GHz

Wireless Gateway
Network Connection . . . . . . 10/100bT Ethernet to SALTO server

Wireless Gateway Power . . . PoE 802.3af or 12V DC

Maximum Locksets per
Wireless Gateway. . . . . 16, can be increased with use of up to 6 wireless nodes, for a maximum of 112 wireless locks per gateway

Encryption, Wireless Gateway
or Node to Lock . . . . AES 128

Encryption, Wireless
Gateway to Server. . . . . SALTO proprietary (based on UDP)

Communications, Wireless
Gateway to Wireless Node. . RS-485 daisy chain

Wiring for Wireless Node
Communication . . . . 6 conductor, CAT 5 twisted pair from Wireless Gateway (2 conductors for data, 4 conductors for power)

Wireless Node Power . . . . . Provided by Wireless Gateway

Wireless range, Gateway or
Node to Lock . . . . 10 - 12m (30 - 35 ft) average, up to 15m (50 ft) max

Wiring distance, Gateway to
First Node . . . . 50m (160 ft) max

Wiring Distance, Node
to Node . . . . 30m (100 ft) max

Wireless Gateway and Hub
Operating Temp Range . . . . . 0° - 60ºC (32º - 140ºF)

Locksets Supporting
Wireless Option . . . . Entire XS4 range (except double sided readers), entire GEO range, Aelement, panic exit devices. Locker locksets cannot be enabled for wireless. Consult SALTO for details.

SALTO Operational Features Supported

	Off-Line Locks	Wireless Locks
Momentary Unlock, Timed (Manual) Unlock from Host	No	Yes, for any wireless lock configured through a Gateway
Scheduled Unlock	Yes	Yes
Lock Down Event	No	Yes
Status Monitoring of Lock and Door Switch	No	Yes
Low Battery Level Alarm	Yes, monitoring and audited on card	Yes, real time
Double Swipe	No	No
Two-Person Rule	Yes, but set up through SALTO software tool	Yes, but set up through SALTO software tool
Area Control/Anti-Passback	Yes, strict and light, but only within SALTO locks	Yes, strict and light, but only within SALTO locks
Clearance Filters	No	No

Related Products

C•CURE 9000

Approvals

CE