



National Protective
Security Authority



AC2000



AC2000 National Protective Security Authority approved

Trusted access control for critical infrastructure

CEM SYSTEMS

Securing mission-critical environments with NPSA assurance

Approved and accredited under the UK National Protective Security Authority (NPSA) Automated Access Control Systems (AACS) scheme, the CEM Systems AC2000 platform delivers trusted, high-assurance access control where security, resilience and operational integrity are critical.

Organisations responsible for government facilities and Critical National Infrastructure (CNI) face increasing physical and cyber security threats. Protecting people, assets and sensitive information requires access control systems that are robust, resilient and independently assured. Working alongside the National Cyber Security Centre (NCSC), the NPSA establishes standards for cyber-secure physical security systems, helping organisations protect critical facilities against increasingly sophisticated threats. AC2000 NPSA has been developed specifically for these high-security environments.

Following successful evaluation under the NPSA AACS scheme, **AC2000 v13.0** has achieved NPSA Assurance and is listed in the NPSA Catalogue of Security Equipment (CSE*).

This recognised accreditation provides confidence that AC2000 v13.0 has been designed, evaluated and maintained in accordance with rigorous NPSA requirements for:

- Hardware Solutions
- System Software
- Installation and commissioning
- Maintenance and support.

AC2000 - BUILT FOR THE MOST DEMANDING ENVIRONMENTS



With more than 35 years of experience securing strategic sites worldwide, and through the design and manufacture of its own hardware and software, CEM Systems has earned a reputation for protecting some of the world's largest and most demanding environments.

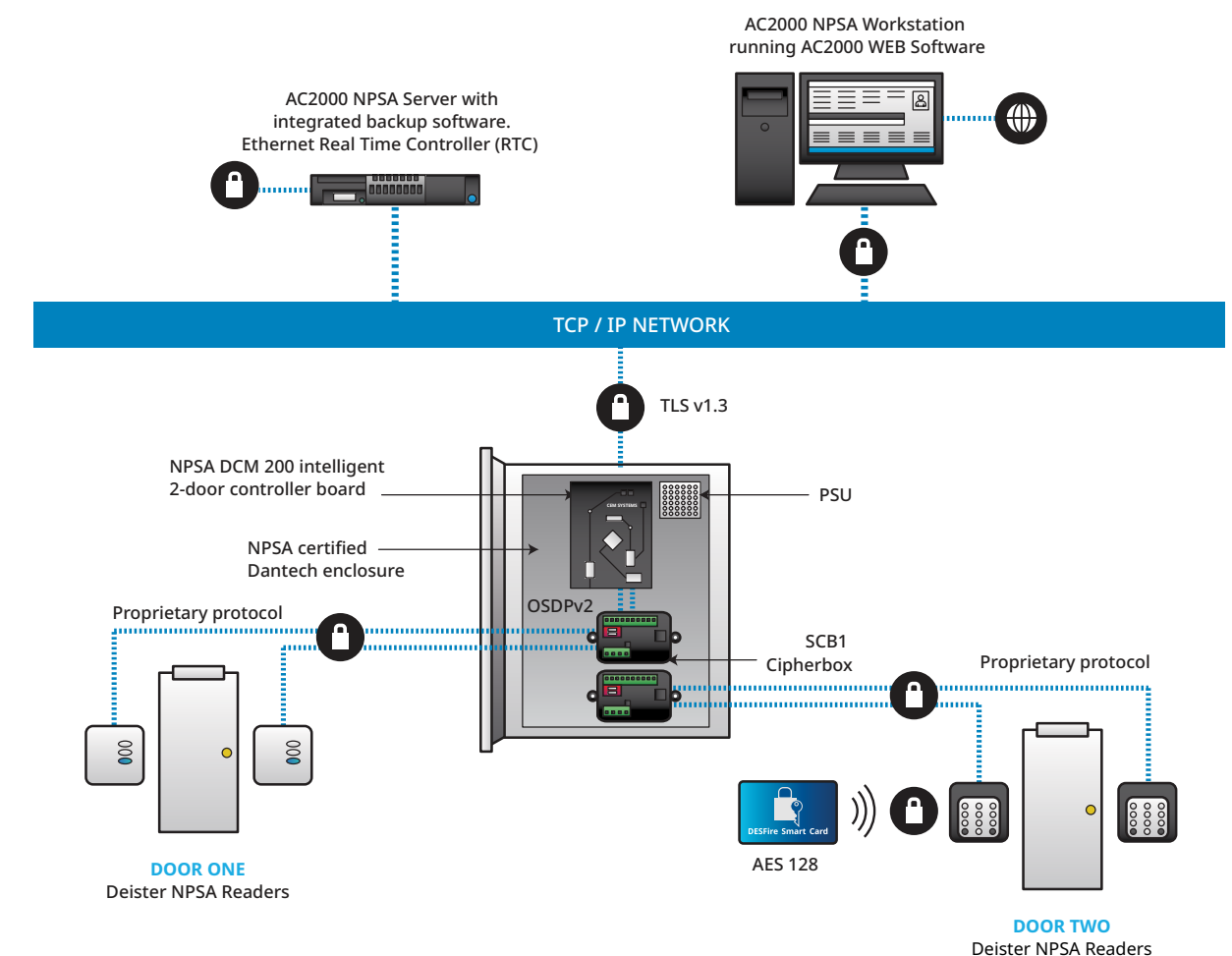
Visit the NPSA website for current product assurance and certification details.

<https://www.npsa.gov.uk>



The AC2000 NPSA-Assured solution combines intelligent hardware, secure web-based software and end to end encrypted communications within an independently evaluated security architecture.

AC2000 V.13.0 NPSA APPROVED SYSTEM OVERVIEW



AC2000 system architecture: End-to-end security

The AC2000 NPSA-Assured platform provides highly secure, end-to-end access control with locked-down protection for system integrity, performance and resilience.

Built on a hardened AC2000 server, tamper-protected workstations, secure web-based administration, intelligent DCM 200 controllers, and encrypted communications, the platform delivers a high-assurance IP access control solution for critical environments. The AC2000 Central Database Computer (CDC) and Real-Time Computer (RTC) server is hosted on NPSA-approved, tamper-protected Dell hardware within a protected enclave, such as a dedicated server room, with operator access restricted to firewall-approved workstations running AC2000 WEB software.



Deployment requirements

To maintain system integrity, the AC2000 NPSA-Assured solution must be installed, configured and commissioned by a CEM Systems AC2000 NPSA Certified Reseller trained and accredited on AC2000 v13.0. All deployment activities must also be undertaken in accordance with NPSA security guidance and mitigation requirements.

Peripheral components, including NPSA-approved readers, keypads, credentials and Request to Exit (REX) devices are required for the complete access control solution but are not included within the AC2000 NPSA AACS evaluation. Assurance for these components is assessed separately through their respective certification schemes.

AC2000 NPSA-Hardened Workstation

Tamper-protected workstation running AC2000 WEB software, enabling system operators to centrally monitor and administer the security system through a secure browser-based interface, accessible only following successful Multi-Factor Authentication (MFA).



AC2000 NPSA-hardened CDC server

Ethernet Real-Time Controller (RTC) with tamper protection & encrypted backup.

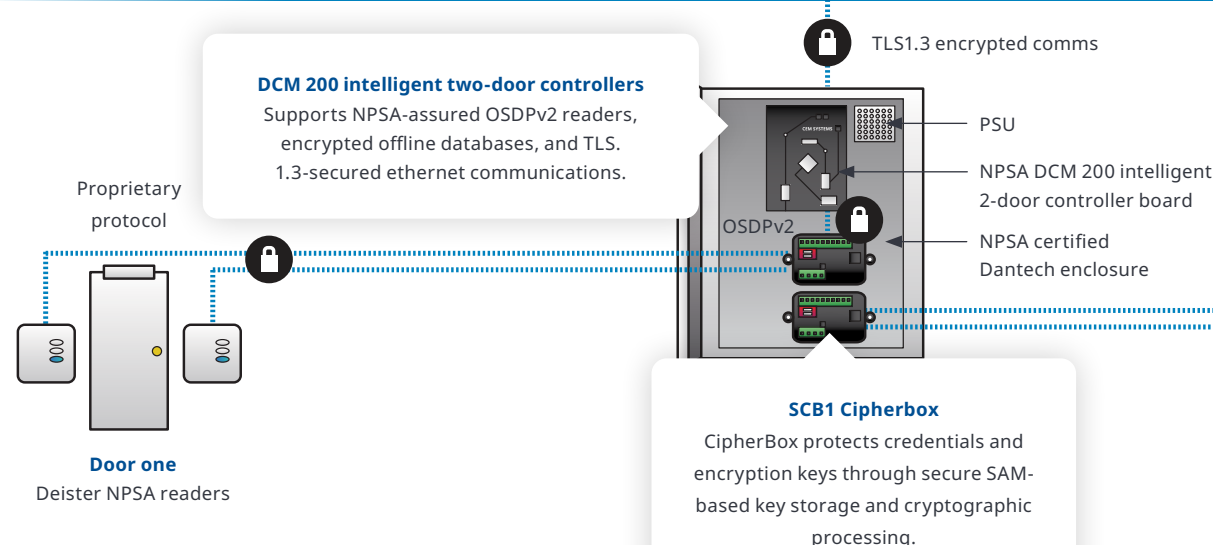


TCP / IP NETWORK

TCP / IP NETWORK

DCM 200 intelligent two-door controllers

Supports NPSA-assured OSDPv2 readers, encrypted offline databases, and TLS. 1.3-secured ethernet communications.



NPSA-certified smart cards

Securely programmed with encrypted keys and enrolled via authorised AC2000 WEB online validation.



AES-128

Door two

NPSA OSDPv2 readers

NPSA-certified OSDPv2 readers

With integrated keypads support card + PIN authentication, AES-128 encrypted communications, and integrated tamper resistance.

DCM 200 intelligent 2-door controller

At the core of the AC2000 NPSA-Assured solution is the CEM Systems DCM 200 intelligent two-door IP controller.

Housed within an NPSA-certified Dantech enclosure and supplied with a CEM power supply unit (PSU) and battery backup, the DCM 200 supports up to four NPSA-certified Open Supervised Device Protocol Version 2 (OSDPv2) smart card readers, enabling bi-directional access control for entry and exit configurations across up to two doors.

The controller features a locked-down encrypted database and incorporates a NIST-certified

FIPS 140-3 cryptographic library to help safeguard critical system data. Powered by high-performance 32-bit processors, the DCM 200 includes an onboard database capable of supporting up to 250,000 cardholders and storing up to 50,000 offline transactions. With full online and offline access decision-making performed locally at the door, the controller ensures uninterrupted operation even when communication with the host server is temporarily unavailable.

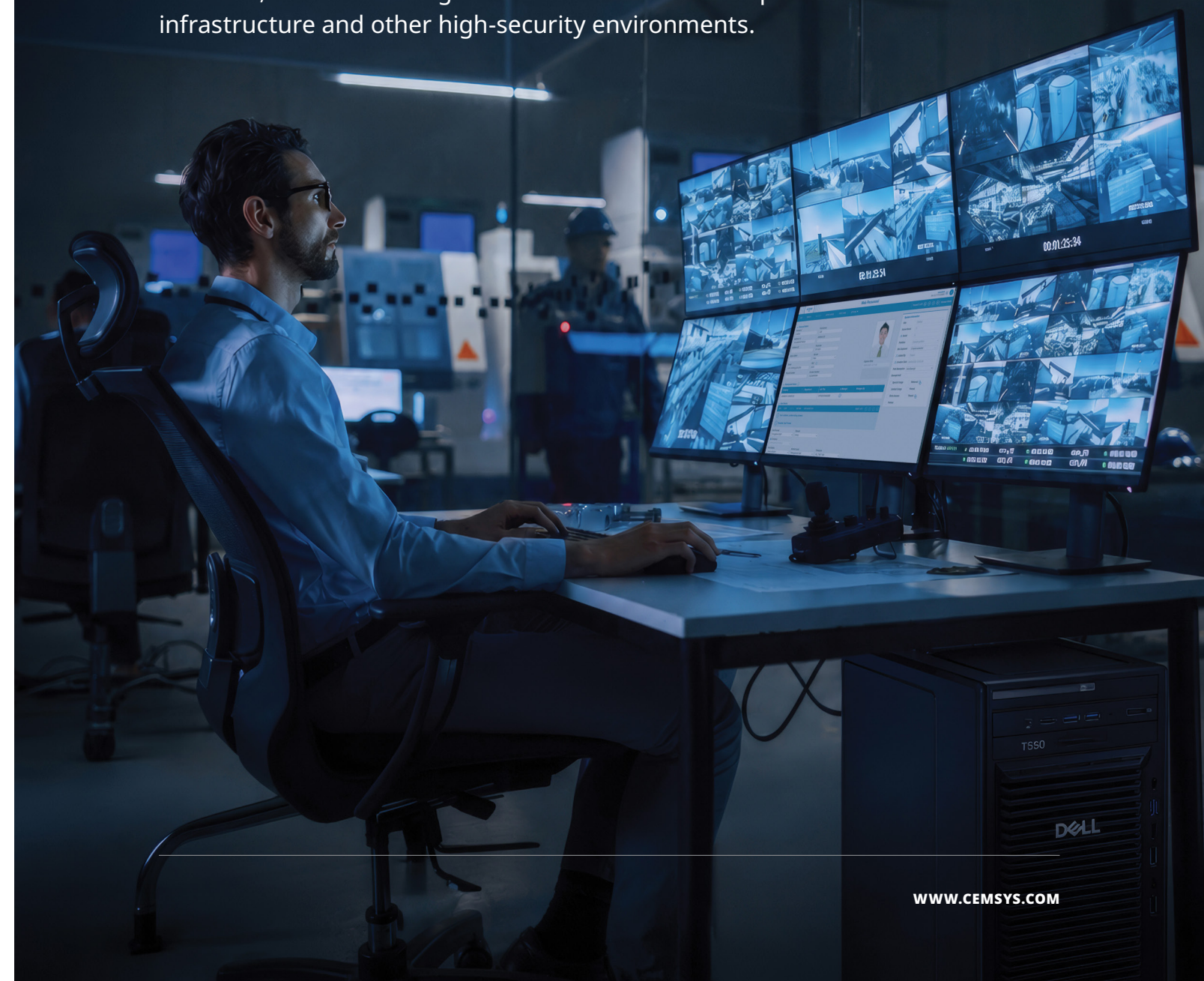
KEY DCM 200 FEATURES

- ✓ Supports up to four OSDP v2 readers (IN/OUT)
- ✓ NIST-certified FIPS 140-3 cryptographic library
- ✓ Unused ports disabled and locked down
- ✓ Secure OSDP v2 communications with AES-128 encryption ensures secure data between readers and controller.
- ✓ Onboard encrypted database with 24/7 offline operation
- ✓ Integrated web dashboard for remote configuration
- ✓ Secure boot, firmware validation and encrypted key storage
- ✓ Local anti-passback functionality
- ✓ Backup power support for operational resilience
- ✓ Automatic lockout following multiple invalid PIN attempts



Secure, distributed architecture

Designed to meet Johnson Controls' highest cybersecurity standards, the AC2000 NPSA-Assured architecture combines distributed intelligence, encrypted communications and local decision-making to maintain operational continuity. AES-128 encrypted OSDPv2 communications help protect against unauthorised interception and credential compromise, while its modular AC2000 v13.0 architecture supports up to 256 doors and can be expanded with additional controllers and software licences as operational requirements evolve, providing a flexible, resilient and high-assurance access control platform for critical infrastructure and other high-security environments.



AC2000 web-based access control



AC2000 WEB delivers a secure, browser-based suite of applications for configuring, monitoring, and administering the AC2000 v13.0 NPSA-Assured system.

The platform provides real-time alarm monitoring, access control administration, personnel and credential management and system and business intelligence analytics/reporting.

By leveraging an intuitive web-based interface on approved and firewall protected NPSA workstations, AC2000 WEB eliminates the need for locally installed client PC software.

Key software capabilities

PERSONNEL, CREDENTIAL & DEVICE MANAGEMENT

- ✔ Supports online smart card validation, batch updates and temporary access assignment.
- ✔ Remote configuration of access control devices and alarm inputs.
- ✔ User-definable software fields to support site-specific operational requirements.
- ✔ Browser-based personnel and cardholder management enables rapid creation, editing, and searching of cardholder records, credential updates, and access assignment.

SECURITY & AUTHENTICATION

- ✔ AC2000 Web incorporates Multi-Factor Authentication (MFA) login with time-based one-time passcodes (OTP) via mobile authentication apps.
- ✔ Role-based AC2000 user permissions provide flexible control over user access to specific system functions.
- ✔ Encrypted backup and recovery capabilities for enhanced resilience and compliance.
- ✔ Supports access levels, time zones, holidays and assignment of temporary access permissions.
- ✔ Rapid site-wide lockdown activation through the web interface.

REPORTING & SECURITY INTELLIGENCE

- ✔ AC2000 Web Reports provide fully customisable reporting for alarms, transactions, device activity and system usage.

REAL-TIME MONITORING & RESPONSE

- ✔ Live online alarm and event monitoring of system events in real time using the AC2000 web interactive alarm event display from a web browser.
- ✔ Alarm filtering, acknowledgement and incident response tools.
- ✔ Zone monitoring and mustering provides live personnel tracking for emergency evacuation management.
- ✔ Instant remote door release using AC2000 Web Oneshot.
- ✔ Simultaneous control of multiple devices using AC2000 Web Broadcast such as opening doors or triggering outputs.
- ✔ Remote adjustment of site security measures during elevated threat levels, including extra PIN checks and restricted cardholder access.



Product codes

SWAC2KNPSA32	AC2000 NPSA Server Software-only Licence for 32 doors
SWAC2KNPSA64	AC2000 NPSA Server Software-only Licence for 64 doors
SWAC2KNPSA128	AC2000 NPSA Server Software-only Licence for 128 doors
SWAC2KNPSA256	AC2000 NPSA Server Software-only Licence for 256 doors
SWAC2KNPSA32-64	AC2000 NPSA Server Software-only Licence Upgrade 32 to 64 doors
SWAC2KNPSA64-128	AC2000 NPSA Server Software-only Licence Upgrade 64 to 128 doors
SWAC2KNPSA128-256	C2000 NPSA Server Software-only Licence Upgrade 128 to 256 doors
DCM/200/NPSA	DCM200 Two Door Controller Module mounted in Dantech enclosure with 12V DC 4A PSU
SSA-NPSA	CEM SSA for AC2000 NPSA system for up 256 devices

NPSA-ASSURED FEATURES AT A GLANCE



High security compliance

Designed to meet stringent UK & US government security standards



Web-based access control

No client software installed – secure, remote configuration



Real-time remote monitoring

Instant alerts and live event tracking via web browser



Scalable architecture

Supports up to 256 secure doors



Intelligent controllers

Offline database & decentralised decision-making for enhanced resilience



System resilience

Ensures 24/7 continuous system operation. Secure OSDPV2 communication with AES encryption



OSDP verified hardware delivers true end-to-end encryption

From readers to devices—protected by FIPS validated components & TLS 1.3 authentication



Advanced reporting

Comprehensive audit trails and analytics for compliance

Request project assistance for AC2000 NPSA

Email emeasecurityproducts@jci.com
or explore more at www.cemsys.com



WWW.CEMSYS.COM

Email emeasecurityproducts@jci.com or follow us @johnsoncontrols

© 2026 Johnson Controls. All rights reserved.

CE1587-BR-202608-R01-A4-EN