



**Product:** [DAC-50](#) 

Software DAC platform with license for 50 AP and 1000 clients

**Product Description**

Software DAC platform with license for 50 AP and 1000 clients

**Technical Specifications**

**Product description**

Type:	DAC-50
Name:	DAC-50
Part Number:	942999321

**Radio technology**

Roaming:	Seamless handover between radio cells; a. On layer 2, DAC supports IEEE 802.11k (Radio Resource Measurement), 802.11v (Wireless Network Management), and 802.11r (Fast Roaming). 802.11k/v enable clients to find the best candidate APs for roaming, while 802.11r optimize association process between Clients and APs. In addition, OKC mechanism is also supported by DAC; b. On layer 3 DAC supports layer 3 roaming by establishing tunnel between AP and Client before roaming happening. Note: 1) IEEE 802.11r is available when using 802.1x authentication or pre-shared keys (PSK) authentication; 2) OKC is available when using 802.1x authentication method only.
Background Scanning:	Background scanning mode enables AP to work intermittently or continuously to maintain normal operation of WIFI system, as well as get as much background information of air-interface as possible, by means of consuming portion of air-interface resources. a. Normal background scanning mode; b. Enhanced background scanning mode, which allows AP to obtain more information on nearby clients and neighboring APs, and the scanning result can be applied by other upper-level applications.
Load Balance:	Load Balance is a systemic mechanism, to provide overall effectiveness of Load balance between different bands of one AP or different APs under one AP cluster. a. 5GHz band steering function, AP will steer more capable clients to 5GHz band where more channel resources are available; b. Under AP cluster, it navigates clients to connecting to the best AP by measuring AP's workload according to quantity of connected clients as well as SNR value (downlink); c. Manual mode allows administrator to adjust specific RSSI value to determine threshold of association and roaming for clients to meet particular requirements.
Automatic Channel Selection:	a. Automatic wireless channel list setting in accordance with each country's regulation; b. Automatic wireless channel bandwidth setting on 2 GHz or 5 GHz according to IEEE 802.11 standard; c. Automatic wireless channel sub-list setting with specified channel list selected by administrator
Automatic TxPower Control:	a. Wireless transmit power on each channel can be automatically controlled by system; b. Wireless transmit power on each channel can be specified as fixed value by administrator; c. Wireless transmit power on each channel can also be specified in a range by administrator
RF Optimization:	RF technology and optimization approaches to improve end-users' experience: a. Single or dual bands is selectable by administrator according to on-site environments; b. QoS (802.1p/DSCP to WMM) on voice and video data to ensure they work on high priority; c. Voice and video services awareness and optimization to ensure their priority is higher than other services; d. Enable Short GI upon better SNR transmission; e. Enable 802.11ax work mode on each band; f. Regularly switch on/off wireless service; g. Allow administrator to limit access from legacy 802.11b/g devices to ensure bandwidth efficiency on 2.4GHz

**Security features**

Portal Server:	a. Support "guest" and "employee" authentication mode; b. DAC provides tailored Portal page template; c. DAC Portal server supports record end-device by MAC address; d. Supports inter-connection with external Portal server;
Access Role Profile:	DAC provides authenticated users by appropriate rights with Access Role Profile. Details as following: a. Administrator can define detailed Policy and Policy list for each Profile; b. Policy supports ACL, while Policy list consist of a group of policies; c. Administrator can define access control rules based on location and period attribute; d. Support QoS attribute likes bandwidth limitation on uplink or downlink for each profile; e. Support VLAN attribute, to assign specific clients into defined VLAN or VLAN pool; f. Access Role Profile function is implemented on AP
Wireless Intrusion Detection System:	DAC provides comprehensive security function to ensure customer wireless cyber security. The system identifies rogue APs by means of following policy and criteria. a. To detect when APs' signal strength threshold exceeds the value defined by administrator; b. To detect if APs' SSID name is valid according to system definition; c. To detect by defined key words (defined by administrator) within SSID name of APs; d. To detect by defined OUI (Organizational Unique Identifier within first six digits of MAC address) of APs, refer to Blacklist mechanism; e. To detect by defined legal OUI, refer to Whitelist mechanism; DAC is also able to detect following cyber-attack behaviors from potential rogue APs or clients: a. APs: AP Spoofing, Broadcast de-authentication, Broadcast disassociation, Ad-hoc network with SSID being used in current infrastructure, invalid long SSID, AP impersonation, Omerta attack, Null probe response, invalid address combination, invalid reason code of de-authentication, invalid reason code of dis-association; b. Clients: Valid Client mis-association, Omerta Attack, Unencrypted Valid Clients, 802.11 40MHz bandwidth intolerance setting, Active 802.11n Greenfield Mode, DHCP client ID, DHCP conflict, DHCP name change, Frequent authentication, long SSID (client), Malformed Frame-Assoc request, invalid reason code of de-authentication, invalid reason code of dis-association;
Wireless Intrusion Prevention System:	In cooperate with WIDS, DAC provides WIPS to implement relevant security policies: a. Security policy to suppress rogue APs to mitigate destructive impacts, by preventing clients from connecting to rogue APs; b. Security policy to suppress rogue clients (active/passive) to mitigate negative effects, by means of blacklist mechanism (static or dynamic); c. Security policy to protect legal equipment by providing whitelist mechanism
Wireless Cyber Security Dashboard:	DAC provide informative dashboard to represent wireless cyber security situation, which is a comprehensive tool to inform user of security status and events. a. Show Rogue APs and channel interference; b. Show Rogue Clients and associated Rogue APs; c. Show Blacklist status of clients; d. Show cyber-attack behavior with details like time record, and etc.
Access Control:	Access control and security mechanism are implemented on AP, a. Stateful IPv4 ACL functionality: Packet filtering in ARP for each authorized Client; b. Layer2 isolation among Clients within one SSID

## Service

Other services:	a. IPv4 : DHCP (Server and Client) only for APs' IP address assignment, Radius (Server, Proxy, Client); LDAP client; AD client; Standard Portal (Portal Server, Portal proxy); Internal Log system; Internal Notification system; External syslog interconnect; Internet standard HTTP API; b. IPv6: only available for data forwarding function on AP; c. ARP and Proxy ARP function on AP
AP Registration:	Users can execute AP registration processes automatically or manually for single device or batch devices. a. Automatic registration by DHCP option; b. Manual registration requires administrator to specify DAC IP address for APs initially working on Cluster mode
Report Generation:	Report system provides online report generation, audit and offline report sending by email address. a. administrator can specify scope of report generation, from Corp-Site-Group; b. administrator can define time interval of reports, including Daily report, Weekly report, and Monthly report; c. administrator can review a report online (on DAC Web UI), or choose to receive a report by email at anytime
Configuration Wizard:	By wizard flow, it is easy for a new user to set up exclusive wireless network from corporation-site-group network scale step by step
Asset Management:	Based on Bluetooth technology on capable AP, DAC provides I/O to interconnect with third-party Asset Management Platform; Note: Bluetooth portable devices, positioning engine, as well as asset management service and application are required

## Software

Switching:	Below data are switching at AP side: a. VLAN IEEE 802.1q, Multicast Snooping (IGMP and MLD), user data per SSID or per ARP (access role profile of clients) b. Support VLAN or VLAN pool c. Data on layer2 are isolated within one SSID
Redundancy:	High availability cluster mode based on K8s platform, with three physical machines for one logical DAC entity, ideal for large scale network deployment
Management:	1. Management interface : HTML5 web interface (HTTPS) and Command Line 2. AP Management : a. Automatically discover the DAC by means of DHCP option 43 b. Manual authentication/registration via web configuration of DAC c. Semi-automatic authentication/registration according to AP list in DAC ('bulk mode') d. DAC can collect APs' notification and log by SYSLOG protocol or internal traps (proprietary protocol) 3. AP Firmware Management : a. Central Firmware deployment (requires external webserver or SFTP server) and management of APs b. Up to date AP firmware version daily checking according to defined policy c. DAC automatically downloads FW from FW server and updates it with required APs.
Time synchronisation:	Activate/inactivate WLAN network (SSID) by time
Routing:	AP supports following routing functions (DHCP server, NAT, DNS proxy) and works as default gateway for clients
Opportunistic Key Caching:	OKC enable clients to perform fast roaming behavior between APs. IEEE 802.1X authentication key between clients and APs is transmitted to all managed APs by DAC.
Radius Server:	A. Authentication and Access Control (Radius Server): a. Support internal and external Radius server; b. Internal Radius server supports Access Role Profile mechanism; c. Authentication methods include: PAP, CHAP, MS-CHAP, MS-CHAPv2, EAP-MD5-Challenge, EAP-GTC, and EAP-MSCHAPv2 B. Software (Radius Server): Radius/EAP Server supports User administration MAC-based, rate limiting, passphrases, VLAN user based, authentication of IEEE 802.1X clients via EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MSCHAP or MSCHAPv2;

## Software requirements

Operating system:	Virtual machine software: VMWare ESXi 6 (or newer) or Microsoft Hyper-V; OS: ubuntu 16.04 server and above
-------------------	--

## Hardware requirements

Hard disk space:	Recommendation: 1T Hard disk, I/O: Input 134MB/s, Output 1.7GB/s
Processor:	Recommendation: 4 core 16G for scale of 50APs+1000 Clients; 8 core 16G for scale of 256APs+5000 Clients; 12 core 32G for scale of 500APs+10000 Clients; 24 core 32G for scale of 1000APs+20000 Clients

## WLAN Access Point

Access Point Functionality:	a. For small network scale with less than 256 APs, APs are able to work under "cluster" mode to achieve self-management; b. For middle/large network scale, APs should be managed by DAC platform in order to perform central management, maintenance and high resilience.
-----------------------------	--

## Scope of delivery and accessories

Scope of delivery:	License Key will be delivered. The License Key is used with the Hardware-ID to request a License File. This License File is used to activate the product Note : DAC-Sec-xxx license is required for Security features
--------------------	---

## History

Update and Revision:	Revision Number: 0.9 Revision Date: 09-07-2023
----------------------	--

© 2023 Belden, Inc

All Rights Reserved.

Although Belden makes every reasonable effort to ensure their accuracy at the time of this publication, information and specifications described here in are subject to error or omission and to change without notice, and the listing of such information and specifications does not ensure product availability.

Belden provides the information and specifications herein on an "ASIS" basis, with no representations or warranties, whether express, statutory or implied. In no event will Belden be liable for any damages (including consequential, indirect, incidental, special, punitive, or exemplary damages) whatsoever, even if Belden has been advised of the possibility of such damages, whether in an action under contract, negligence or any other theory, arising out of or in connection with the use, or inability to use, the information or specifications described herein.

All sales of Belden products are subject to Belden's standard terms and conditions of sale.

Belden believes this product to be in compliance with all applicable environmental programs as listed in the data sheet. The information provided is correct to the best of Belden's knowledge, information and belief at the date of its publication. This information is designed only as a general guide for the safe handling, storage, and any other operation of the product itself or the one that it becomes a part of. The Product Disclosure is not to be considered a warranty or quality specification. Regulatory information is for guidance purposes only. Product users are responsible for determining the applicability of legislation and regulations based on their individual usage of the product.