HIRSCHMANN
A BELDEN BRAND

Product: DAC-Sec-1000

Software DAC platform security features license for 1000 AP

Product Description

Software DAC platform security features license for 1000 AP

Technical Specifications

Product description

Name:	DAC-Sec-1000
Part Number:	942999330

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

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