# Cisco Wireless Controller 5508 (WLC)

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics** | **Scenarios** | **Testing Criteria** | **Results** |
| **WLC** | Verification of Successful mounted in the rack. |  |  |
| Verify that power supply is working |  |  |
| 802.11 a/g Complaint |  |  |
| 802.11n |  |  |
| Automates wireless configuration and management functions denial-of-service attacks, Management frame protection detects malicious users and alerts network administrators. |  |  |
| Complaint Centralized security policy |  |  |
| RF Management |  |  |
| Must be integrate-able with access points installed over LAN and WAN at remote sites |  |  |
| Wireless Standards Support: IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n |  |  |
| Wireless intrusion prevention system Capability |  |  |
| Must support VLAN Trunking so that a client access network from anywhere will be able to get same rights to network |  |  |
| Wired/Switching/ Routing: IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T. 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q Vtagging, and IEEE 802.1AX Link Aggregation. |  |  |
| RF Interference Mitigation |  |  |
| Security Standards: WPA ● IEEE 802.11i (WPA2, RSN) ● RFC 1321 MD5 Message-Digest Algorithm ● RFC 1851 The ESP Triple DES Transform ● RFC 2104 HMAC: Keyed Hashing for Message Authentication ● RFC 2246 TLS Protocol Version 1.0 ● RFC 2401 Security Architecture for the Internet Protocol ● RFC 2403 HMAC-MD5-96 within ESP and AH ● RFC 2404 HMAC-SHA-1-96 within ESP and AH ● RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV ● RFC 2406 IPSec ● RFC 2407 Interpretation for ISAKMP ● RFC 2408 ISAKMP ● RFC 2409 IKE ● RFC 2451 ESP CBC-Mode Cipher Algorithms ● RFC 3280 Internet X.509 PKI Certificate and CRL Profile ● RFC 3602 The AES-CBC Cipher Algorithm and Its Use with IPSec ● RFC 3686 Using AES Counter Mode with IPSec ESP ● RFC 4347 Datagram Transport Layer Security ● RFC 4346 TLS Protocol Version 1.1 |  |  |
| Encryption Support: WEP and TKIP-MIC: RC4 40, 104 and 128 bits (both static and shared keys) ● AES: CBC, CCM, CCMP ● DES: DES-CBC, 3DES ● SSL and TLS: RC4 128-bit and RSA 1024- and 2048-bit ● DTLS: AES-CBC ● IPSec: DES-CBC, 3DES, AES-CBC |  |  |
| Authentication, Authorization and Accounting (AAA):  ● IEEE 802.1X ● RFC 2548 Microsoft Vendor-Specific RADIUS Attributes ● RFC 2716 PPP EAP-TLS ● RFC 2865 RADIUS Authentication ● RFC 2866 RADIUS Accounting ● RFC 2867 RADIUS Tunnel Accounting ● RFC 2869 RADIUS Extensions ● RFC 3576 Dynamic Authorization Extensions to RADIUS ● RFC 3579 RADIUS Support for EAP ● RFC 3580 IEEE 802.1X RADIUS Guidelines ● RFC 3748 Extensible Authentication Protocol ● Web-based authentication ● TACACS support for management users |  |  |
| Management: SNMP v1, v2c, v3 ● RFC 854 Telnet ● RFC 1155 Management Information for TCP/IP-Based Internets ● RFC 1156 MIB ● RFC 1157 SNMP ● RFC 1213 SNMP MIB II ● RFC 1350 TFTP ● RFC 1643 Ethernet MIB ● RFC 2030 SNTP ● RFC 2616 HTTP ● RFC 2665 Ethernet-Like Interface types MIB ● RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual Extensions ● RFC 2819 RMON MIB ● RFC 2863 Interfaces Group MIB ● RFC 3164 Syslog ● RFC 3414 User-Based Security Model (USM) for SNMPv3 ● RFC 3418 MIB for SNMP ● RFC 3636 Definitions of Managed Objects for IEEE 802.3 MAUs |  |  |
| Primary requirement of authentication will be from Domain Active Directory however proposed solution must also support authentication from third party RADIUS Server |  |  |
| Provision of N+1 redundancy for higher availability |  |  |
| Multiple Gigabit interfaces |  |  |
| Client Load Balancing |  |  |
| Dynamic Power Transmit Control |  |  |
| Make sure that Product is not End of Sale or end of life |  |  |
| Provision of controlling access points over WAN links |  |  |
| Make sure that Product is not refurbished |  |  |
|  |  |  |
|  |  |  |
| Check both the SFP port is working in active/ backup mode. | Go to Controller and plug out one of the cable connected to management port,  Browse the controller got to controller tab and click on interfaces now click any interface and note that the active port is 2. |  |
| Check the Management port IP | From the Controller Summary |  |
| Verify the network connectivity of WLC. | Ping from the controller right top corner to any network accessible IP. |  |
| Verify Successful acceptance of AP. | Go to tab click Access Points ->All APs |  |
| Verification of License of WLC with 50 APs. | Management tab --> Software Activation--> Licenses. |  |
| Support for reliable streaming video and toll quality voice | Browse the WLC  Wireless --> media stream |  |
| Cross network access to real-time and historic RF interference. | Browse the WLC  Monitor -->Cisco CleanAir  -->802.11b/g -->Interference Devices |  |
| Latest Software version | From the Controller Summary |  |
| Communication b/w APs, Controller, WCS and MSE. | Ping APs IP, WCS and MSE through Controller |  |
|  | Roaming of Wireless clients from one AP to another AP without connection drop. A WLAN Enabled SIP Phone moving from one AP range to another AP range during a call must be smoothly handoff without call drop, same true for video and data connections. | Connect the laptop to the SSID and walk to the next Near AP it will Roam and ping any IP of the networks. |  |
| Check the adaptive power management to turn off access point radios during off peak hours. | Browse WCS  Wireless --> TPC |  |
| Support Rogue AP detection. | From the Controller Summary |  |
| Verify that Wireless clients will get same access rights, IP Address and will remain member of same VLAN while moving from one AP range to another or having new connection with any of the installed APS | Connect the laptop to the SSID check the IP and move towards the next AP range and check again the laptop IP it will remain same. |  |
| Check that authentication all wireless clients from AD accounts | Browse the ACS  [:2002](http://10.10.250.29:2002)  Go to external data base -->windows database--> check that your AD is there click on it --> Add mapping here you find the AD groups from where the users authenticated. |  |
| WLAN Enabled SIP phone MAC Authentication. | Browse the WLC    click the security tab -->  MAC Authentication |  |
| Alarm detail and Summary | From the Controller Summary |  |
| Security Standards: WAP, WAP2, WEP, TKIP, AES and AAA (802.1X). | Browse the ACS  [:2002](http://10.10.250.29:2002)  Global Authentication |  |
| Management: SNMP V1, V2c, V3 | Browse the WLC    management --> SNMP |  |
| Check the Clean Air technology is working. | Browse WCS  Wireless -->802.11b/g/n  -->CleanAir |  |
| Check the Remote AP is connected and broadcast the SSID and users are Associates with it. | Browse the WLC    wireless tab. |  |
| Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network.Mesh is working | Browse WLC  Wireless --> Mesh |  |
| Dynamic Channel Assignment | Browse the WLC    wireless --> 802.11b/g/n  --> DCA |  |
| Support RF Visibility and Protection | Browse WCS  MAP |  |
| Separate SSIDs | Browse the WLC    WLAN |  |
| Clients Load balancing | Browse the WLC    wireless --> Advance -->Load Balancing |  |
| Latest Software Version | http://www.cisco.com/cisco/software/release.html?mdfid=282600534&flowid=7012&softwareid=280926587&release=7.0.220.0&relind=AVAILABLE&rellifecycle=ED&reltype=latest |  |
|  | Support 200 APs and 3000 clients | http://www.cisco.com/en/US/products/ps10325/index.html |  |
| Real time communication b/w AP, WLC and WCS | Browse the WLC    Monitor --> Summary  Here you find the running communication b/w AP Auth. Server.  Or  From WCS |  |
| Larger mobility domain for more simultaneous client associations, Faster RRM updates for uninterrupted network access when roaming, Intelligent RF control plane for self-configuration, self-healing, and selfoptimization, Efficient roaming to improve application performance such as toll quality, voice, and consistent streaming video and data backup | Browse the WLC    Wireless -->802.11b/g/n  --> RRM --> Roaming |  |
|  | CAPWAP AP to control encryption. | Browse the WLC    wireless --> All AP  select the Remote AP and check that Encryption is Enable. |  |
| WIPS | Browse the WLC    wireless --> All AP  Select one of the AP and set  AP Sub Mode |  |
| RF Management | Browse the WLC    Wireless -->802.11b/g/n  --> RRM |  |
| QOS | Browse WLC    WLAN --> QOS |  |
| Secure tunnels with AP | By Using CAPWAP tunnel and LWAPP commands |  |
|  | Total WLC Ethernet Modules Throughput must support 50 APs throughput |  |  |
| All Licenses must on name of |  |  |
| Datasheet and Complete Documentation |  |  |
|  |  |  |

# Cisco APs

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics** | **Scenarios** | **Testing Criteria** | **Results** |
| **CISCO APs** | 802.11n Complaint | Browse WLC  Wireless--> Access Point--> Radios--> 802.11b/g/n |  |
| 802.11b/g Complaint | Browse WLC  Wireless--> Access Point--> Radios--> 802.11b/g/n |  |
| 802.11 a Complaint |  |  |
| IEEE 802.11n Compliant (2.4 & 5 GHz) |  |  |
| Data and signaling encryption with support of DES, 3DES and AES Encryption algorithm |  |  |
| Must be controller based access points for centralized authentication, policy management, Configuration, encryption and all in centralized topology |  |  |
| Must support 802.11n migration service |  |  |
| Must have latest software version |  |  |
| Must support WLAN Performance and Security assessment |  |  |
| Must support Dual Radios (2.4GHz and 5GHz Frequency Bands) |  |  |
| Excellent transmit power |  |  |
| High Memory |  |  |
| PoE Enabled |  |  |
| Must support centralized authentication via centralized controller and integrate with Domain Microsoft active directory for authentication using domain accounts. |  |  |
| All Access Points must be able to connect with controller via wired as well as wireless network. |  |  |
| These APs will be installed as indoor so vendor must provide external antennas to have maximum coverage inside building |  |  |
| APs must support adoption of 802.11n in mixed-client networks by making sure that 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries. |  |  |
| Proposed APs must have bandselect feature |  |  |
| Vendor must provide mount kits for all proposed equipment |  |  |
| Controller based network management |  |  |
| Must be able to detect malicious users and alerts network administrators |  |  |
| Dynamic Frequency Selection 2 (DFS-2) compliant |  |  |
| Proposed APs must support all WLAN Services like WLAN Planning and Design, WLAN 802.11n Migration Service, WLAN Performance and Security Assessment etc |  |  |
| EAP Type(s):Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), Protected EAP (PEAP) v0 or EAP-MSCHAPv2, Extensible |  |  |
| Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), PEAPv1 or EAP-Generic Token Card (GTC), EAP-Subscriber Identity Module (SIM) |  |  |
| Integrated Antennas: 4 dBi Gain (2.4 GHz), 3 dBi Gian (5 GHz) |  |  |
| Certified by WiFi Alliance (802.11 a/b/g/n & WMM) |  |  |
| Support for Zero-Touch-Configuration |  |  |
| Wireless Client will get same access rights, IP Address and will remain member of same VLAN while moving from one AP range to another or having new connection with any of the installed APs. |  |  |
| Prevention against DHCP spoof attacks |  |  |
| Make sure that Product Model is not end of sale or end of life |  |  |
| Make sure that Product is not refurbished |  |  |
| Data and signaling encryption | Browse WLC  Wireless --> All AP select the AP --> Advance tab  Data Encryption |  |
| Support Centralized planning and designing services. | Browse WCS  Maps |  |
| Support transmission of Voice, Video and Data | Browse WLC    Wireless--> QOS  Browse WLC    WLAN -->802.11b/g/n -->  Media |  |
| QOS test | Browse WLC    WLAN --> QOS |  |
| Support Multicast | Browse WLC    Controller -->  Multicast |  |
|  | Rogue APs detection | Browse WLC    Monitor -->  Rogue AP |  |
| Detect Rogue users | Browse WLC    Monitor --*>*  Rogue Clients |  |
| Support all WLAN Services Like WLAN Planning and Design. | Browse WCS    MAP |  |
| Mobility | Browse WLC    Controller -->Mobility Management  Or  Connect the laptop to the SSID and walk to the next Near AP it will Roam and ping any IP of the networks. |  |
| Supports 802.1X, WPA, WPA2, AES, TKIP, WEP, 802.1x, MIC, IEEE 802.11 WEP keys of 40 bits and 128 bits | Browse WLC    WLAN --> Security tab |  |
| Support Wi-Fi Multimedia WMM | Browse WLC    WLAN --> QOS  --> WMM |  |
|  | Support VLAN Trucking | CLI |  |
| APs have management console and Ethernet port. |  |  |
| Must Support Control and Provisioning of Wireless Access Points compliant DTLS encryption to ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links. | Browse WLC    Wireless --> All APs --> select any AP --> Advance  --> Data Encryption |  |
| wireless standards support b/g/n/e/d/h/a | 802.11e It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions.  802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate  802.11h is intended to resolve interference issues |  |
|  | Support VLAN Trunking | Management port is trunk therefore it support VLAN Trunking  CLI: Show interface Vlan |  |
| Support IEEE 802.1Q and 1000 Base-T SFP port | Browse the WLC    Controller -->  Ports |  |
| Security Standards:  WAP2, WAP, MD5, HMAC-MD5, HMAC-SHA, CBC-DES, AES-CBC, | MD5 --> Management -->  SNMP V3 User-->  Authentication protocol and Privacy protocol |  |
| Encryption Support:  WEP, TKIP-MIC | WLC    WLAN -->  Security |  |
| Throughput test |  |  |
|  | Datasheet and Complete Documentation |  |  |

# Cisco MSE 3310

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics** | **Scenarios** | **Testing Criteria** | **Results** |
| **MSE Hardware/Software** | Check the MSE is mounted. |  |  |
| Check that MSE is working. |  |  |
| Check that MSE is integrated with WCS. | Browse WCS  --> services --> Synchronization History |  |
| Check the license of MSE. | Browse WCS  --> Administration --> License Center --> MSE |  |
| WIPS profile includes  Denial of Service Attack  DOS Attack Against AP  DOS Attack Against infrastructure  DOS Attack Against Station  WIPS Security Penetration | Browse WCS  --> Configure  --> WIPS Profile |  |
| Show data under clients -> Clients detected by MSE |  |  |
| Verify That MSE has latest software version |  |  |
| Verify that WIPs has latest signatures |  |  |
| Verify that WIPs update signature from internet |  |  |
| All Licenses must on name of |  |  |
| Datasheet and Complete Documentation |  |  |

# WCS

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics** | **Scenarios** | **Testing Criteria** | **Results** |
| **WCS** | Check the WCS is installed. |  |  |
| Management platform for lifecycle management of 802.11n and 802.11a/b/g wireless networks |  |  |
| Automatically mitigating the impact of radio frequency (RF) interference |  |  |
| Able to manage more than 10 x Wireless LAN controllers |  |  |
| 802.11n access points |  |  |
| Capability to manage more than 1000 APs |  |  |
| Support wireless mobility services and adaptive wireless intrusion prevention systems (wIPS) |  |  |
| Controller configurations, updates, and scheduling across the entire wireless network. Auto-provisioning access points, with easy-touch templates that support customized configuration of single or multiple access points. |  |  |
| Maintenance, security, troubleshooting, and future capacity planning activities |  |  |
| Quick access to actionable data of Wireless network |  |  |
| Check the integration of WLC and MSE. | Browse WCS  --> Configure  --> Controllers |  |
| Access to critical information, faults, and alarms based on their severity; facilitating faster assessment of outstanding notifications and supporting quicker resolution of trouble tickets. Detecting, locating, and containing unauthorized (rogue) devices is fully supported when location services are enabled |  |  |
| Able to quickly identify, isolate, and resolve problems across all components of the Wireless Network. Supports rapid troubleshooting of any size WLAN. |  |  |
| Quickly assess service disruptions, receive notices about performance degradation, research resolutions, and take action to remedy no optimal situations. Integrated workflows with support of seamless linkage between all tools, alarms, alerts, searches, and reports for all infrastructure components and client devices. |  |  |
| Discover nonoptimal events occurring outside baseline parameters such as client connection or roaming problems. Search tool to immediate and historic information about devices and assets located anywhere in the wireless network. |  |  |
| Finding, classifying, correlating and mitigating sources of interference from Wi-Fi and non-Wi-Fi sources such as rogue access points, microwave ovens, Bluetooth devices and cordless phones. Creates a self-healing, self-optimizing wireless network that mitigates the impact of wireless interference sources. |  |  |
| Troubleshooting tool for step-by-step method to analyze problems for all client devices to help reduce operating costs by speeding the resolution of trouble tickets for a variety of Wi-Fi client device types. Specialized diagnostic tools to support enhanced analysis of connection |  |  |
| Centralized Security and Network Protection: Wireless security solution must integrate security alerts, alarms, adaptive wireless intrusion prevention system  (wIPS) and technology into a single unified platform, from a centralized view. ● Must provide critical information about RF interferes that are potential security threats. ● Robust adaptive wIPS supports quick detection, location, and containment of unauthorized (rogue) devices ● Protect against unauthorized intrusion and RF attacks ● Automated alarms for rapid responses to mitigate risks ●Supports multiple unique service set identifiers (SSIDs) with customizable security and enforcement parameters ● Management frame protection to monitor the authentication of 802.11 management frames ● Access point wired port authentication with 802.1X to validate all access point credentials ● Tuning of access points on or off at scheduled intervals. ● Unified wired and wireless security by integration with Self-Defending Network and Network Admission Control (NAC) |  |  |
| Rack mounted Computer System, Operating system and all other required software for installation of Wireless Control and Monitoring System |  |  |
| Software must be latest version |  |  |
| Provided System must have compatible and licensed operating system |  |  |
| Check the license of WCS. | Browse WCS  --> Administration --> License Center --> WCS |  |
| All APs are Present in WCS | Browse WCS  --> Configure  --> Access Points |  |
| Check that how many Clients were Authenticated by using EAP or OPEN | Browse WCS  Client |  |
| Check that MSE is detecting threats/Attacks | Browse WCS  Security |  |
| Plan, Deploy, Monitor and Reports on indoor and outdoor wireless networks | Browse WCS  Plan and Monitor and Report Tabs |  |
| Support WIPS | MSE |  |
| Planning and design tools for defining access point placement and determining access point coverage areas for standard and irregularly shaped buildings which help to eliminate improper RF designs and coverage problems. | Browse WCS  Maps |  |
|  | Clear visibility into RF environment, air quality, and air quality information to anticipate future coverage needs, and assess wireless LAN events | Browse WCS  Maps |  |
| Integrated configuration templates and deployment tools | Browse WCS  Configure > Access Point Templates. |  |
| Alarm detail and summary | Alarm Summary Page for WCS |  |
| Check the latest software | http://www.cisco.com/cisco/software/release.html?mdfid=279705270&catid=278875243&softwareid=280926613&release=7.0.220.0&relind=AVAILABLE&rellifecycle=ED&reltype=latest |  |
| O/S compatible | Windows 2003 server  Red Hat Enterprise Linux 5 server  http://www.cisco.com/cisco/software/release.html?mdfid=279705270&catid=278875243&softwareid=280926613&release=7.0.220.0&relind=AVAILABLE&rellifecycle=ED&reltype=latest |  |
| Classifying, correlating and mitigating sources of interference from Wi-Fi and non Wi-Fi sources. | WCS --> Configuration --> Interference |  |
|  | AP on and off at scheduled intervals | WCS -->  AP/Radio Templates  Go Green |  |
| Customizable reporting to assists IT teams in more effectively manners. | WCS -->  Reports |  |
| All Licenses must on name of |  |  |
| Datasheet and Complete Documentation |  |  |
| Provided WCS System must have all OS Patches and latest software version |  |  |

# Cisco ACS 4.2

|  |  |  |  |
| --- | --- | --- | --- |
| **Topics** | **Scenarios** | **Testing Criteria** | **Results** |
| **ACS 4.2** | Check that ACS Authenticate users that are present in the AD as well as in the ASC databases. |  |  |
| Check that the ACS using the Domain Certificate. |  |  |
| ACS defines the respective VLAN to the Users or Groups. |  |  |
| All Licenses must on name of |  |  |
| Datasheet and Complete Documentation |  |  |
| Provided ACS System must have all OS Patches and latest software version |  |  |

# 