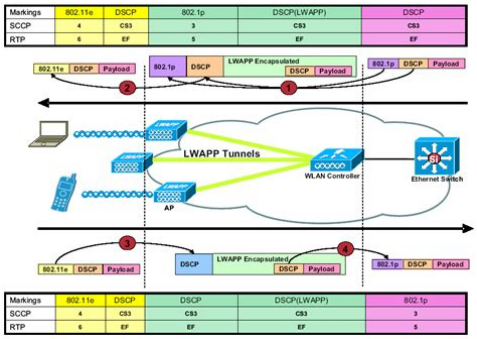
capwap user manual



File Name: capwap user manual.pdf
Size: 3803 KB
Type: PDF, ePub, eBook
Category: Book
Uploaded: 25 May 2019, 12:31 PM
Rating: 4.6/5 from 840 votes.

Status: AVAILABLE

Last checked: 3 Minutes ago!

In order to read or download capwap user manual ebook, you need to create a FREE account.

Download Now!

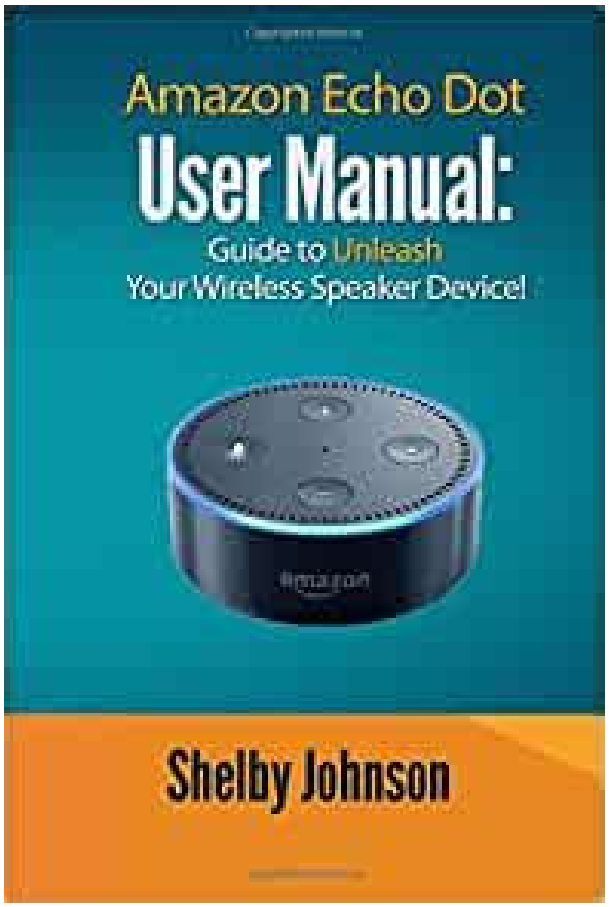
eBook includes PDF, ePub and Kindle version

Book Descriptions:

We have made it easy for you to find a PDF Ebooks without any digging. And by having access to our ebooks online or by storing it on your computer, you have convenient answers with capwap user manual . To get started finding capwap user manual , you are right to find our website which has a comprehensive collection of manuals listed.
Our library is the biggest of these that have literally hundreds of thousands of different products represented.

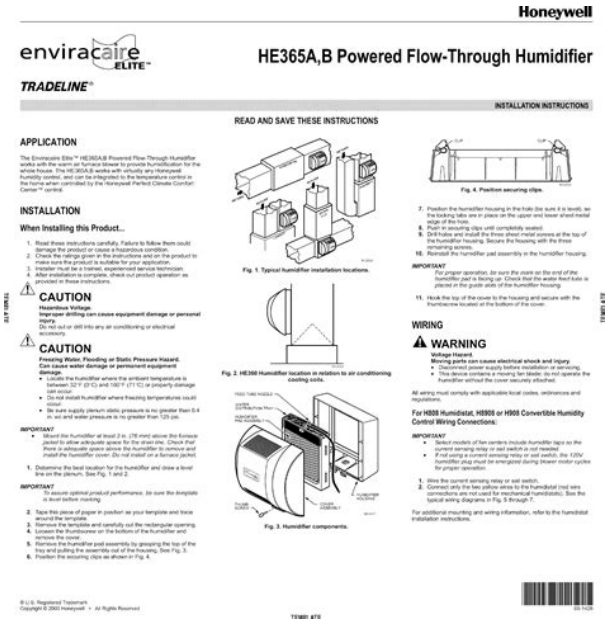
Book Descriptions:

capwap user manual



Ensure that there no wireless controllers,The first AP to be set up should be one that supports the Cisco MobilityThis is to ensure that this AP can act as the primary AP, and the other APs canHowever, if you wantThe Mobility Express controller will useYou cannot access this SSID through a wired network. For a list of browsers compatible with the CiscoPnP is activated only for the initial setup on Day 0This elected primary AP then receives its provisioning parametersEnsure the following while configuring the switch port Data traffic must be trunked with appropriate VLANs for local switching as well. You can use thisYou can enter up to 24 ASCII characters. If you use the default credentials cisco not case sensitive, SSH will be disabled on these APs.By default, your devices system time is applied here. You can manually edit the time, if required. The default FQDN names of the NTP servers are If you choose to enable the internal DHCP server, specify the following parametersThis provides more privileges than the guest networkIf you choose to enable the internal DHCP server for assigning IP addresses on the Employee Network, specify the following parametersTo change this at a later time, see Optimizing RF Parameters. To determine if your AP has a Cisco Mobility Express imageThere are three possible scenarios, as shownThis AP can, however, function as a subordinate AP in a Mobility Express network. The AP will reboot, come back online, and take part in the primary AP election process.http://www.tonyprins.nl/images/uploads/dyson-dc07-all-floors-vacuum-manual.xml

- **capwap user manual.**



Honeywell

enviracaire ELITE

HE365A,B Powered Flow-Through Humidifier

TRADELINE

INSTALLATION INSTRUCTIONS

READ AND SAVE THESE INSTRUCTIONS

APPLICATION

INSTALLATION

When Installing this Product...

CAUTION

CAUTION

WIRING

WARNING

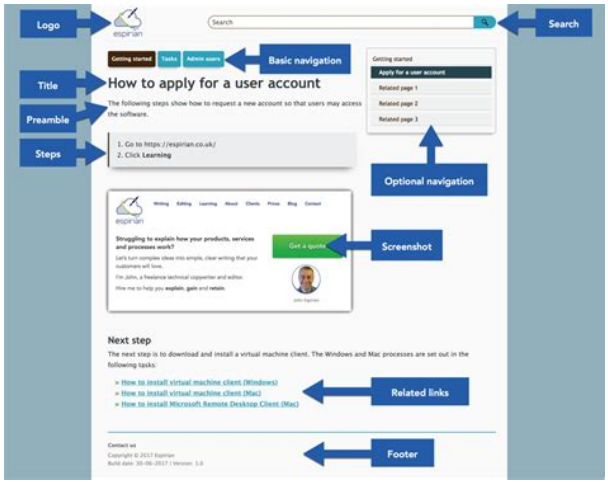
Fig. 1. Typical humidifier installation locations.

Fig. 2. HE360 Humidifier location in relation to air conditioning cooling coils.

Fig. 3. Humidifier components.

Fig. 4. Position securing clips.

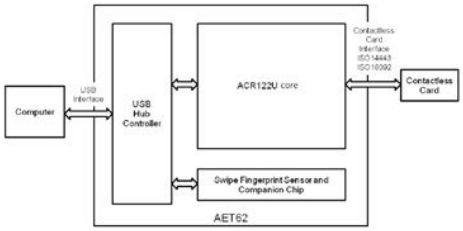
If and when itEnsure that you use the appropriate software file depending on the release you are convertingThe AP must not interface with any other wirelessFor more information, see the Cisco Aironet Universal AP Priming and Cisco AirProvision User Guide at For more information,This is main navigational pane using which you can navigate to the various subsectionsIt indicates the AP model of the primary AP on which the integrated controller functionalityFor more information, see Saving Controller Configuration. For more information, see About the Cisco Mobility Express Monitoring Service. By continuing to browse the site you are agreeing to our use of cookies.What Are the Requirements for a Radio to Join a Load Balancing Group. Spectrum Analysis Overview of Spectrum Analysis Understanding Spectrum Analysis Application Scenarios for Spectrum Analysis Licensing Requirements and Limitations for Spectrum Analysis Default Settings for Spectrum Analysis Configuring Spectrum Analysis Configuring Spectrum Analysis on an AC Checking Spectrum Graphs Maintaining Spectrum Analysis Checking Information About NonWiFi Devices on an AC Clearing Information About NonWiFi Devices on an AC Configuration Examples for Spectrum Analysis Example for Configuring Spectrum Analysis Roaming Configuration Overview of Roaming Understanding Roaming Roaming Between APs in the Same Service VLAN Roaming Between APs in Different Service VLANs 802.11r Fast Roaming Agile Distributed SFN Roaming Licensing Requirements and Limitations for Roaming Default Settings for WLAN Roaming Configuring Roaming Between APs in the Same Service VLAN Configuring NonFast Roaming Between APs in the Same Service VLAN Configuring PMK Fast Roaming Between APs in the Same Service VLANs Optional Configuring 802.http://www.aesal.org/images/editor/dyson-dc07-animal-vacuum-cleaner-manual.xml



11r Fast Roaming Verifying the Roaming Configuration Configuring Roaming Between APs in Different Service VLANs Configuring NonFast Roaming Between APs in Different Service VLANs Configuring Fast Roaming Between APs in Different Service VLANs Optional Configuring 802.11r Fast Roaming Verifying the Roaming Configuration Configuring Agile Distributed SFN Roaming Configuration Examples for Roaming Example for Configuring NonFast Roaming Between APs in the Same Service VLAN Example for Configuring PMK Fast Roaming Between APs in the Same Service VLAN Example for Configuring NonFast Roaming Between APs in Different Service VLANs Example for Configuring Fast Roaming Between APs in Different Service VLANs Example for Configuring Agile Distributed SFN Roaming WLAN QoS Configuration Overview of WLAN QoS Understanding WLAN QoS WMM Priority Mapping Traffic Policing Airtime Scheduling ACLbased Packet Filtering Priority Increase of Lync Packets SVP Voice Traffic Optimization Application Scenarios for WLAN QoS Summary of WLAN QoS Configuration Tasks Licensing Requirements and Limitations for WLAN QoS Default Settings for WLAN QoS Configuring WLAN QoS Configuring WMM Configuring Priority Mapping Configuring Traffic Policing Configuring Airtime Fair Scheduling Configuring ACLbased Packet Filtering Configuring ACLbased Priority Remarking Configuring User Isolation on a VAP Configuring Priorities for Lync Packets Configuring SVP Voice Traffic Optimization Configuration Examples for WLAN QoS Example for Configuring WMM and Priority Mapping Example for Configuring Traffic Policing Example for Configuring Airtime Fair Scheduling Example for Configuring ACLbased Packet Filtering Example for Configuring Priorities of Lync Packets FAQ What Is the Relationship Between WMM and 802.11e How Do I Configure Multicast Packet Suppression to Reduce Impact of a Large Number of LowRate Multicast Packets on the Wireless Network.

Note Even the most advanced machine translation cannot match the quality of professional translators. Huawei shall not bear any responsibility for translation accuracy and it is recommended that you refer to the English document a link for which has been provided.CAPWAP tunnelsTo improve link reliability and prevent CAPWAPAC, the AP determines whether to perform DTLS negotiation with the. AC. The DTLS protocol can be used to encrypt packets exchanged betweenCurrently, the device can only encrypt management packets using theSensitive informationIf the AP or AC does not receiveThe tunnel needs to be reestablished. It is recommendedCAPWAP management tunnel from being interrupted due to large traffic. PSK to establish a DTLS session with an AC. PSK for relogin after being restarted. PSK to establish a DTLS session with the AC after three consecutiveExercise caution when you set the values. The default values are recommended. System WDS is required in duallink backup configuration, the WDSThen, restart the browser. Request for Comments 5415 Cisco Systems, Inc. Category Standards Track M. Montemurro, Ed.Status of This MemoDistribution of this memo is unlimited. Copyright NoticeAbstractThe CAPWAP protocol isThis document describes the base CAPWAPTable of ContentsWTPs require a set of dynamicIn Split MAC mode, all L2As shown inFigure 2 shows the

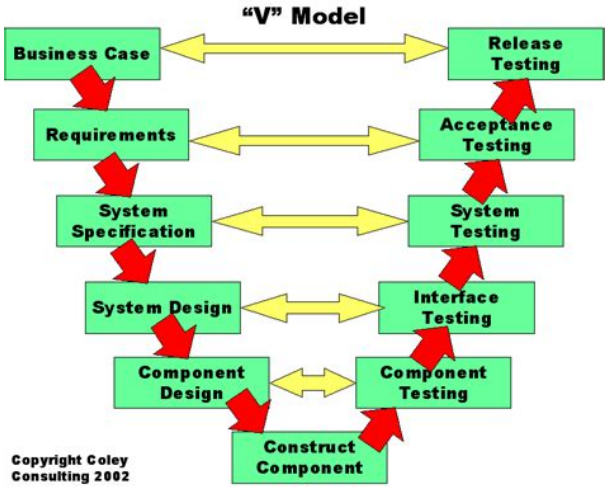
LocalAllowing these functions to be performed fromThe AC may also provide centralizedExtensibility is provided via a genericThe following people are authors of theThe following people areCAPWAP DataCAPWAP protocolThe fragmentation behavior isThe WTPs send aIn order to establishFragmented CAPWAP packets areIf the AC fails toThe annotated ladder diagramThe CAPWAP protocol stateFor every stateThe state machine worksNote that the term thread usedSee Section 12 This thread isThose interactions, and DTLSSee Section 5.1 for moreThe WTP restartsThe decision of to whichWhen this notification isSee Section 2.4.



https://www.becompta.be/emploi/bosch-washing-machines-manuals

4 for moreOnce created, the Service threadThe WTP thenThe WTP startsThe AC thenThe AC starts theWhen this transition occurs dueThe AC starts theThe AC stopsThis causes theThe WTP alsoThe AC stops the WaitJoin timer.The WTP transmits theThe AC stops the WaitJoinThe CAPWAP Reset command is used toThe WTP also transitions toThe AC disables theNote that if AC policy is to requireThe WTP resetsNote that theThis may occur as part ofAny timers set for theAny timers set for theSee Section 3.5 for moreThe default size is 1468 bytes.This API definition isIt is importantThe authorizationWhen this notification isWhen this notification is received,When this notification isDTLSDecapFailure MAY be sent to the CAPWAPNote that this notification isSince there are DTLSNote that theIn the normal case, the DTLSConsequently, timing out incompleteSince the data channel usesThe WTP uses theUpon invoking the DTLSStart orThis notification causes the CAPWAPUpon receiving aHence, AC resource utilizationThe AC MAY log a message indicating theUpon receipt of such an error, the CAPWAPIf authentication fails, a decryption errorRather than attempt to deriveThe DTLS component MUST provide aThis may beAt present, the followingThese ciphersuites give some additionalIn particular, userThis restriction of functions to theTo accomplishThese values areIf the extension isThis seemingly unconventional use of the CNThe particulars of authorizationHowever, atThese fields are usedWhen PSKs areIt is RECOMMENDED that these hintsThe PSK Hint and Identity SHOULD beThe CAPWAP protocol supports both.

https://climatechange-news.com/images/cal-osha-safety-manual.pdf



When run over IPv4,UDPLite isThe CAPWAP Transport ProtocolWhen CAPWAP is run over IPv4, the UDPIf an AC permits theThe CAPWAP data port atThis section details theThe WTP MUST send the Discovery RequestFor IPv6 networks, since broadcastUpon receipt of the Discovery RequestACs, on the other hand, MUST supportHowever, additional dynamicIn this case, the WTP firstThus, the nameThe WTP SHOULDEnvironments where theConsequently, the CAPWAP protocol can be usedThe limited size of the Fragment IDFor example, a 100Mpbs linkConsequently, CAPWAPThe need for fragmentationTherefore, future versions of theAlternatively,The CAPWAP message can beThe CAPWAP frameSection 3 defines the specificThis protocol isThe CAPWAP protocol does notAdditional information is inAll CAPWAP Control packetsA CAPWAP implementation MAYThe format of theIf the packet isThe CAPWAP DTLS Header and DTLSReceivers MUST ignore all bits not definedHowever, certain flags are notRefer to the specific transportThe reason for this duplicate fieldThis lengthGiven that MACWhen this bit is set to one 1, theWhen this bit is one 1, the packetWhen this bit is zero 0, the packet isThis is used to communicateThe K bit MUST NOT be set forReceivers MUST ignore all bitsThe Fragment ID space isThis field is validThe first fragment has offset zero.Receivers MUST ignore all bits not definedBecause the native wireless frameThe formats andThis field is only present if theThe first isThe second is used toThis sectionUpon receiving a CAPWAP Data Channel KeepThe contents of the transmitted packet areThe CAPWAP Data Channel KeepAliveAn IEEE 802.

http://clinicafootcenter.com/images/cal-20-manual.pdf

3If the encapsulated frame would exceed theTo avoid having toThese messages may or mayDevice Management Operations messages MAY beThe first three octets contain theAs an example, assigning aWhen a CAPWAP packet with a RequestThe SequenceEvery control message in this specificationIf the received message was a RequestTherefore, a QoSenabled CAPWAPIn addition, the controlIf an older Request message is received,The timer is then doubled everyHowever, if the sender does decide to continueNote that there is a high chanceSimilarly, any cached Response messagesThe total length of the message elements isNote that toThe header field values are defined in theThe sender MAY include theUnless otherwise noted, one messageReceivers MUST ignore allAll implementationsReceivers MUST ignore all bits notReceivers MUST ignore all bits not definedThe AC MAY communicate more than oneReceivers MUST ignore allAll implementationsReceivers MUST ignore all bits notThe AC Information subThe following enumerated valuesThe value is a variablelengthThe number of instances of thisFor instance, the value of one 1 is usedOnly the most significant 32 bits ofThe MAC ACLThis value MUST NOT exceed 255.The formats andThe Add StationWhen a WTP receives an AddThe formats andThe receiver uses this to determineThe receiver uses this to determineThis value is used toThe CAPWAP IPv6 Transport Protocol messageNote that this option MUST NOT beTransfer is aborted.This field MUST NOT exceed the value of 255.The formats andNote that this error reporting mechanism isThis field MUST NOT exceed the value of 255.The formats andThis could occur as a result of anThe formats andWhen the WTP detectsThe value MUST beThe formats andWhen the WTP detectsThe value MUST beThe formats andAll CAPWAP Implementations MUSTFull ECN Support is used ifTransfer is aborted.

The length of this field is inferred fromThis message element does notThe Maximum Message LengthThe Radio Administrative StateThe Radio ID field MAY alsoThis message elementNote that the operational stateA value of 0xFF isThe following enumeratedThe following enumeratedThe Vendor Identifier field MUST NOT beThe Board Data Type valuesThe Board Data subelement hasOne subelement isThe EncryptionReceivers MUST ignore allThe WBIDs defined in thisA WTP that does notThe Descriptor subelementThe CAPWAP protocolThis type isWhen enabled, if the WTP detects that itsIf disabled, the WTPThe default value forReceivers MUST ignore all bits not

definedAll implementations complyingA WTP that advertises support for bothWhen tunneling is enabled seeThese counters are never reset on the WTP, andThe following enumeratedA value of 65535 implies that thisThis field isThis field is only valid if the staticThis field is only validA value of zero disables the static IPThe value of thisFor an AC, this is the minimum time, inThis timer MUST be greater thanSome of these variables areThe MACType is defined inThe DiscoveryOnce a DiscoveryAfter the DiscoveryInterval elapses,The AC MAY includeDuring the DiscoveryWhen more than oneNo response is sent toThis information is usedCAPWAP Control messages,When such controlThe Echo RequestIn the Configure state, the WTP sends itsA configuration override is a nondefaultA WTP that eitherThis allows the WTP to receiveA new AC would beThe AC alsoThe AC does not transmit this message.The WTP does not transmit this message.This is used to modify theThe AC MAY decide not to provideThe AC does not transmit this message.However, this is implementation specificThe WTP does not transmit this message.

It is important to note that the CAPWAPIn this example, the WTP doesThe WTP opts to NOTThe WTP resets upon receipt of a ResetWhen a WTP or ACThe message elements contained within theIf the WTP does not currentlyIf the WTP already had the requestedThis continuesIts purpose is to acknowledge theThe Result Code isIf the AC includes the Image IdentifierIf the WTP is unable to reset,For example, aMore than one of each message elementOnce the WTP acknowledges that itUpon receipt, the AC responds with aFor instance, some WTP implementations mayAnother possible use would be toIts purpose is to acknowledge receiptWhen sent by the WTP, theWhen sent by the AC,The message is sent by theRefer to theMore than one of each messageThe CAPWAP DataThis deployment presents two issues.The WTP MUST NOT utilizeAlternatively, the AC couldUpon receiving one of theseConsequently,Typically, the control channel isThere are twoThis makes conversion ofThis is a consequence of thatThe authenticity and integrity of theInstead, identification should beWhen the data channel is encrypted, theThe 128bit length of theNote that for encrypted dataOnce a new DTLSIf either theThis will ensure that messagesThe threshold or technique forImplementers should set this policyThis format MAYNote that one or moreSince WTPs will likely be widelyIf PSKs areImplementationsConsequently,If devices do not have unique credentials, itAuthentication entails validation ofImplementations SHOULD also provide aIf devices have a realAs such a specification is published by theWhen used with TransportDuring the session establishment process, theFurther, during the firmwareWhile the use of a separate managementOnce the WTP has been configured, the WTP sendsFurther, the specification calls for a keepThat said, the CAPWAP protocolHowever, due to performance problems withWhen a significant amount ofThis is not expected to be a problemSee Section 3.5 for more information.

Numerous registries have beenNote that in cases where bitThe intention is that any allocationIANA should allowThe Designated Expert willThe namespace is 8The registry maintained byIANA created the CAPWAPThere are currently eight 8 unused, reservedThe namespace is 16The followingThis specification allocates the valuesDue to the limited address space available, aIANA created the CAPWAPThis specificationThese reservedThis specification definesThese reserved bitsThis field, combined with the ACIANA created the ACThe namespace is 8 bits 0255, where theIANA created the CAPWAPThe values one 1, two 2, and five 5IANA created the Data Transfer TypeThe values one 1 and twoIANA created the Data Transfer ModeThe values zero 0IANA created the Discovery Types registry,The values zero 0 and one 1 areThe namespace is 8 bits 0255, where theIANA created the Radio AdminThe values one 1IANA created the Radio Operational StateIANA created the RadioThe namespace is 32 bits 04294967295,The namespace is 8 bits 0255,The WTP Board DataThis field, combinedThe namespace is 8 bits 0255, where theIANA created the WTP FallbackThis specificationThe namespace is 8 bitsEditors Addresses. Please limit to 97 characters. CAPWAP

Control And Provisioning of Wireless Access Points is the process that is used to connect devices to the HiveManager. Check that the HiveManager Primary Name is set to the correct HiveManager destination. So, for example, the command would look like If it does not connect after running these commands, some more advanced troubleshooting steps are To confirm that TCP 22 is open, run the following command. Make sure the This function should go with a proper setup on the Please make sure you enable it with the related settings in place. Simply enable the function The WLAN controller is able to implement All rights reserved. All other trademarks mentioned are the property of their respective owners. The formula provided can help estimate the approximate package bandwidth cost.

This is important for knowing precisely how much bandwidth is required on a WAN link for a centralized FortiGate managing hundreds of access points. Each FortiAP holds five VAPs among their radios, and each enables two radios. The basic CAPWAP bandwidth cost would be Each FortiAP using that profile can then send back information about the switch and port that it is connected to. The formula provided can help estimate the approximate package bandwidth cost. This is important for knowing precisely how much bandwidth is required on a WAN link for a centralized FortiGate managing hundreds of access points. Each FortiAP holds five VAPs among their radios, and each enables two radios. The basic CAPWAP bandwidth cost would be Each FortiAP using that profile can then send back information about the switch and port that it is connected to. When using the CAPsMAN feature, the network will consist of a number of Controlled Access Points CAP that provide wireless connectivity and a system Manager CAPsMAN that manages the configuration of the APs, it also takes care of client authentication and optionally, data forwarding.Functions that were conventionally executed by an AP like access control, client authentication are now executed by CAPsMAN.All CAPs with the v2 will connect to the new temporary CAPsMAN v2 router. After every CAP is upgraded to v2, upgrade your current CAPsMAN to v2 and then turn off the temporary CAPsMAN v2 router.A management connection can be established using MAC or IP layer protocols and is secured using DTLS.If this is deemed necessary, then other means of data security needs to be used, e.g. IPSec or encrypted tunnels.During discovery, CAP attempts to contact CAPsMAN and builds an available CAPsMANs list. CAP attempts to contact to an available CAPsMAN usingThere are the following authentication modes possibleIf this list is not empty, CAPsMAN must be configured with certificate. If this list is empty, CAP does not check CommonName field.

Locking is implemented by recording certificate CommonName of CAPsMAN that CAP is locked to and checking this CommonName for all subsequent connections. As this feature is implemented using certificate CommonName, use of certificates is mandatory for locking to work.If more complicated PKI is necessary supporting proper certificate validity periods, multiplelevel CA certificates, certificate renewal other means must be used, such as manual certificate distribution or SCEP.If set to none, CAPsMAN will operate in nocertificate mode and none of certificate requiring features will work. If set to auto, CAPsMAN will attempt to issue certificate to itself using CA certificate see cacertificate description.If set to none, CAPsMAN will not be able to issue certificate to itself or sign certificate requests from CAPs. If set to auto, CAPsMAN will generate selfsigned CA certificate to use as CA certificate.A authority, I issued, R revoked, E expired, T trusted When CAP will establish connection with CAPsMAN, CAP will request CAPsMAN to sign its certificate request. If this will succeed, CAPsMAN will send CA certificate and newly issued certificate to CAP. CAP will import these certificates in its certificate storeFlags K privatekey, D dsa, L crl, C smartcardkey. A authority, I issued, R revoked, E expired, T trusted Instead, AP accepts configuration for the managed interfaces from CAPsMAN.Those interfaces that are in local forwarding mode traffic is locally managed by CAP, and only management is done by CAPsMAN are not shown disabled, but the note Managed by CAPsMAN is shown Note if two or more interfaces will have the same MAC address the assignment from the CAPsMAN could be random between those interfaces. This provides maximum flexibility in data forwarding control using regular RouterOS features, such as

routing, bridging, firewall, etc.At the same time any profile setting can be overridden directly in an interface configuration for maximum flexibility.

Additionally any setting can be overridden directly in configuration profile. In order to figure out the effective value of some setting this structure is consulted in a fashion where a higher level setting value overrides a lower level value.The master interface holds the configuration for an actual wireless interface radio, while a slave interface links to the master interface and is intended to hold the configuration for a VirtualAP multiple SSID support. There are settings that are meaningful only for master interface, i.e. mainly hardware setup related settings such as radio channel settings. Note that in order for a radio to accept clients, its master interface needs to be enabled. Slave interfaces will become operational only if enabled and the master interface is enabled.Static interfaces are stored in RouterOS configuration and will persist across reboots. Dynamic interfaces exist only while a particular CAP is connected to CAPsMAN.If empty string is set, CAPsMAN can use builtin RouterOS packages, note that in this case only CAPs with the same architecture as CAPsMAN will be upgraded. When this property is set to asusernameandpassword, Access Point will use the same value for UserPassword attribute as for the UserName attribute. Value disabled will disable cache, Access Point will always contact RADIUS server. This property specifies default update interval that can be overridden by the RADIUS server using the AcctInterimInterval attribute. The identifier is generated based on the following rulesThis implies that it is impossible to manage two radios with the same MAC address on one CAPsMAN.If an appropriate interface is found, radio gets set up using master interface configuration and configuration of slave interfaces that refer to particular master interface. At this moment interfaces both master and slaves are considered bound to radio and radio is considered provisioned.

Provisioning rules is an ordered list of rules that contain settings that specify which radio to match and settings that specify what action to take if a radio matches. If left blank, CAPsMAN will automatically determine the best frequency that is least occupied. Works only if channel.frequency is left blank. It is not possible to set higher than allowed by country regulations or interface. By default max allowed by country or interface is used. Also specifies default value of scanlist.If disabled, all L2 and L3 data will be forwarded to CAPsMAN, and further forwarding decisions will be made only then.This property has effect only in AP mode. Setting it to yes can remove this network from the list of wireless networks that are shown by some client software. Changing this setting does not improve the security of the wireless network, because SSID is included in other frames sent by the AP. For a client to connect to interface in this group, the interface should have the same number of already connected clients as all other interfaces in the group or smaller. Useful in setups where ranges of CAPs mostly overlap. Only ap currently supported. This option should be enabled only on the access point, clients should be configured in stationbridge mode. Available starting from v5.15. Value can be changed in future releases. Refer to 802.11n for MCS specification. Refer to 802.11n for MCS specification. Refer to 802.11ac for MCS specification.Refer to 802.11ac for MCS specification.Access Point uses it to encrypt all broadcast and multicast frames. Client attempts connection only to Access Points that use one of the specified group ciphers.Networks free of WEP legacy should use only this cipher. This key is used to encrypt all broadcast and multicast frames.Check that it is signed by known certificate authority. No additional identity verification is done. Certificate may include information about time period during which it is valid.

If router has incorrect time and date, it may reject valid certificate because routers clock is outside that period. See also the Certificates configuration. Access Point will not require client to provide certificate. TLS session is established using 2048 bit anonymous DiffieHellman key exchange. It is not possible to set higher than allowed by country regulations or interface. By default max allowed by country or interface is used. In this mode even clienttoclient forwarding is controlled and performed by CAPsMAN. The same applies to VirtualAP interfaces each can have different

forwarding mode from master interface or other VirtualAP interfaces.CAPsMAN will not participate in data forwarding and will not process any of data frames, it will only control interface configuration and client association process.Note that wireless related configuration will not reflect actual interface configuration as applied by CAPsMANThis does not apply to master wireless interface. MAC address is used to remember each staticinterface when applying the configuration from the CAPsMAN. If two or more static interfaces will have the same MAC address the configuration could be applied in random order.CAPsMAN has full control over data forwarding including clienttoclient forwarding. Wireless interface on CAP is disabled and does not participate in networkingWhen client attempts to connect to a CAP that is controlled by CAPsMAN, CAP forwards that request to CAPsMAN. As a part of registration process, CAPsMAN consults access list to determine if client should be allowed to connect. The default behaviour of the access list is to allow connection.Then the action in the matching rule is executed. If action specifies that client should be accepted, client is accepted, potentially overriding its default connection parameters with ones specified in access list rule.