ArubaOS 6.1
Command Line Interface

ARUBA networks

eference Guide

Copyright

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

ARUBA®
networks

www.arubanetworks.com

1344 Crossman Avenue
Sunnyvale, California 94089

Phone: 408.227.4500
Fax 408.227.4550

The ArubaOS command line interface (CLI) allows you to configure and manage your controllers. The CLI is accessible from a local console connected to the serial port on the controllers or through a Telnet or Secure Shell (SSH) session from a remote management console or workstation.

NOTE

Telnet access is disabled by default. To enable Telnet access, enter the telnet cli command from a serial connection or an SSH session, or in the WebUI navigate to the **Configuration > Management > General** page.

What's New In ArubaOS 6.1

The following commands have been added in the ArubaOS 6.1 command line interface.

Command	Description
`clear wms wired-mac`	Clear *learned* and *collected* Wired MAC information.
`cluster-member-custom-cert`	This command sets the controller as a control plane security cluster root, and specifies a custom user-installed certificate for authenticating cluster members
`cluster-member-factory-cert`	This command sets the controller as a control plane security cluster root, and specifies a custom user-installed certificate for authenticating cluster members.
`controller-ipv6`	This command sets the default IPv6 address of the controller to the IPv6 loopback interface address or a specific VLAN interface address.
`crypto-local ipsec sa-cleanup`	Issue this command to clean IPsec security associations (SAs).
`crypto-local isakmp certificate-group`	Issue this command to configure an IKE Certificate Group for VPN clients.
`crypto-local isakmp sa-cleanup`	This command enables the cleanup of IKE SAs.
`crypto-local isakmp xauth`	This command assigns the server certificate used to authenticate the controller for VPN clients using IKEv2.
`ip igmp`	Added parameters: `max-members-per-group` and `quick-client-conver`
`interface vlan ipv6 address`	This command configures the link local address or the global unicast adress for this interface.
`ipv6 cp-redirect-address`	This command configures a redirect address for captive portal.
`ipv6 default-gateway`	This command configures an IPv6 default gateway.
`ipv6 mld`	This command configures the IPv6 MLD(Multi-listener discovery) parameters.
`ipv6 neighbor`	This command configures an IPv6 static neighbor on a VLAN interface.
`ipv6 route`	This command configures static IPv6 routes on the controller.

Command	Description
local-custom-cert	This command configures the user-installed certificate for secure communication between a local controller and a master controller.
local-factory-cert	This command configures the factory-installed certificate for secure communication between a local controller and a master controller.
netdestination6	This command configures an alias for an IPv6 -only network host, subnetwork, or range of addresses.
netexthdr	This command allows you to edit the packet filter options in the extension header (EH).
ntp authenticate	This command enables or disables NTP authentication.
ntp authentication-key	This command configures a key identifier and secret key and adds them to the database. NTP authentication works with a symmetric key configured by user. The key is shared by the client (Aruba controller) and an external NTP server.
ntp trusted-key	This command configures an additional subset of trusted keys which can be used for NTP authentication.
remote-node-local-factory-cert	Configure factory certificates for secure traffic between Remote-Node-Masters and Remote-Nodes.
show controller-ipv6	This command displays the controller's IPv6 address and VLAN interface ID.
show ipv6 interface	This command displays IPv6-related information on all interfaces.
show ipv6 neighbors	This command displays the IPv6 neighbors configured on a VLAN interface.
show ipv6 route	This command displays the controller IPv6 routing table.
show local-cert-mac	Display the IP, MAC address and certificate configuration of local controllers in a master-local configuration.
show netexthdr	This command displays the IPv6 extension header (EH) types that are denied.
show wms wired-mac	Display a summary table of Wireless Management System (wms) wired MAC information.
tracepath	Traces the path of an IPv6 host.

Modified Commands

The following commands were modified in ArubaOS 6.1.

Command	Parameter Description
aaa authentication captive-portal black-list <black-list> | white-list <white-list>	Name of an existing black list or white list on an IPv4 or IPv6 network destination. The black list contains websites (unauthenticated) that a guest cannot access. The white list contains authenticated websites that a guest can access.
aaa authentication-server radius source-interface <vlan>	Associates a VLAN interface with the RADIUS server to allow the group-specific source interface to override the global configuration.
aaa derivation-rules user <name> set {role|vlan} condition dhcp-option	Use DHCP signature matching to assign a role or VLAN to a specific device type.

Command	Parameter Description
aaa profile <profile> devtype-clasification	When the devtype-classification parameter is enabled, the output of the **show user** and **show user-table** commands shows each client's device type, if that client device can be identified
aaa profile <profile> enforce-dhcp	When you enable this option, clients must complete a DHCP exchange to obtain an IP address.
aaa profile <profile> radius-interim-accounting	By default, the RADIUS accounting feature sends only start and stop messages to the RADIUS accounting server. Issue the interim-radius-accounting command to allow the controller to send Interim-Update messages with current user statistics to the server at regular intervals.
aaa authentication via connection-profile admin-logoff-script | admin-logon-script	Use this option to specify scripts that must be executed after VIA connection is established and terminated.
aaa authentication via connection-profile ikev2-policy | ikev2-proto | ikev2auth | ipsecv2-cryptomap	Use this option to enable IKEv2 authentication mechanism.
aaa authentication via connection-profile suiteb-crypto	Use this option to enable Suite B cryptography support.
clear	Clears all IPv6 session statistics, multicast listener discovery (MLD) group and member information, MLD statistics, and counters. The following MLD parameters are added to the **ipv6** option: ● mld group ● mld stats-counters
cluster-root-ip ipsec-factory-cert| ipsec-custom-cert	The **ipsec-factory-cert** and **ipsec-custom-cert** parameters were introduced to allow certificate-based authentication of cluster members.
crypto dynamic-map set pfs group19|group20	The **pfs** parameter was modified to support the group19 and group20 PFS group values.
crypto ipsec transform-set <transform-set-mtu> esp-aes128-gcm |esp-aes256-gcm	This command configures IPsec parameters. ● Use ESP with 128-bit AES-GCM encryption. ● Use ESP with 256-bit AES-GCM encryption.
crypto isakmp eap-passthrough eap-mschapv2|eap-peap|eap-tls	Select one of the following authentication types for IKEv2 user authentication using EAP.
crypto isakmp policy authentication ecdsa-256	Use ECDSA-256 signatures for IKE authentication.
crypto isakmp policy authentication ecdsa-384	Use ECDSA-384 signaturesfor IKE authentication.
crypto isakmp policy hash sha1-96	Use SHA1-96 as the hash algorithm.
crypto isakmp policy hash sha2-256-128	Use SHA2-256-128 as the hash algorithm.
crypto isakmp policy hash sha2-384-192	Use SHA2-384-192 as the hash algorithm.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.