Technology Solution Guide

Deploying Ascom Myco with Aruba Networks’ Secure Mobility Solution

Ascom Myco
Software version 1.6.0

Aruba 600/3000/6000/7000/7200 Mobility Controllers
AOS version 6.4.2.5


April 7th 2015
WARRANTY DISCLAIMER

THE FOLLOWING DOCUMENT, AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "AS IS" BASIS. ARUBA MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

DISCLAIMER OF LIABILITY

Aruba Networks, Inc. disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the certification program or the acts or omissions of any company or technology that has been certified by Aruba Networks.

Certification does not mean that the company is a subcontractor or under the technical control or direction of Aruba Networks. In conducting the certification program Aruba Networks is not undertaking to render professional or other services for or on behalf of any person or entity.
Table of Contents
Introduction .................................................................................................................................................. 3
Solution Components .................................................................................................................................. 3
    Aruba Campus WLAN Solution .............................................................................................................. 3
    Ascom Solution .................................................................................................................................. 4
ArubaEdge Solution Qualification ............................................................................................................. 6
    Qualification Objective ......................................................................................................................... 6
    Network Topology ................................................................................................................................. 6
    Test Methodology ................................................................................................................................. 8
    Summary Test Results ............................................................................................................................ 8
    Know Limitations ................................................................................................................................. 10
Conclusion ................................................................................................................................................... 10
Appendix 1 .................................................................................................................................................. 11
    General settings (SSID, Radio and QoS) ............................................................................................... 11
    Encryption and Authentication Settings ............................................................................................... 15
    Ascom Myco Setting Summary ............................................................................................................. 18
APPENDIX B ................................................................................................................................................. 22
    Test Summary ..................................................................................................................................... 22
    Aruba Test Configuration File ............................................................................................................ 23
Introduction
This document describes the steps and guidelines necessary to configure Aruba’s wireless LAN (AOS version. 6.4.2.5) infrastructure to work interoperable with Ascom’s Myco handsets.

The guide is intended to be used in conjunction with Aruba and Ascom configuration guides. Please contact the respective company’s sales engineering or support groups should additional information be required.

Solution Verified: Ascom Phones
Aruba Product: Aruba Campus WLAN Solution OS version 6.4.x.x
Partner Solution Tested: Ascom Myco Handset; Software version 1.6.0

Solution Components

Aruba Campus WLAN Solution
Secure and reliable mobility is the responsibility of the enterprise network, which must support a wide range of converged clients over wireless, wired, and remote access networks. Laptops and smartphones are capable of simultaneously running voice, data, and now video applications, an operating model that breaks traditional dedicated VLAN and SSID architectures. Delivering the quality of service (QoS), bandwidth, and management tools necessary to accommodate these devices on a grand scale – within a campus environment, to users on the road, and in branch offices – requires a specially tailored system design.

Aruba’s unique application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to ensure highly reliable application delivery. Aruba’s integrated policy enforcement firewall isolates applications from one another to essentially create multiple dedicated virtual networks, and then allocates the necessary bandwidth for each user and application.

To ensure reliable application delivery in changing RF environments, Aruba’s Adaptive Radio Management (ARM) technology forces client devices to shift away from the noisy 2.4GHz band to the quieter 5GHz band, adjusts radio power levels to blanket coverage areas, load balance by shifting clients between access points, and even allocates airtime based on the capabilities of each client device. The result is a superb user experience without any user involvement.

These services are complemented by security systems that ensure the integrity of the network. Rogue detection, wireless intrusion and prevention, access control, remote site VPN, content security scanning, end-to-end data encryption, and other services protect the network and users at all times.
Aruba’s extensive portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to unified communications applications and services - regardless of the user's device, location, or network. This dramatically improves productivity, lowering capital and operational costs while providing a superior uninterrupted user experience.

**Ascom Solution**

Nurses are the everyday heroes in healthcare and deserve their very own companion to assist them in their jobs – that's why we developed Ascom Myco® (My companion). It is a truly purpose-built smartphone for healthcare, providing caregivers and clinicians with the information they need where it matters the most – at the heart of care.

**Key Benefits**

- Highly ergonomic design: compact, lightweight and optimized for single hand usage.
- Durable and robust: built from materials specifically designed to withstand excessive drops and corrosion from disinfecting agents.
- Built on open software standards (for integration with other systems and to support 3rd party apps), with addition of Ascom mission-critical extensions for information security.
- Specially designed carrying clip evenly distributes weight and provides a firm grip on a single layer of fabric to prevent drops.
- Every Ascom Myco comes with Product Protection Service including one stop for technical support, free updates and upgrades. Extend your coverage with Silver or Gold Product Protection Service

**USPs**

- Top Display for "At a Glance" notifications.
- Prioritized mission-critical Apps.
- Patient-centric user experience.
- Fully centralized management.
- Compact, lightweight, and highly ergonomically design.
- Durability.
## Certified Product Summary

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Ascom Wireless Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Products Certified</td>
<td>Ascom Myco</td>
</tr>
</tbody>
</table>

- **Hardware Model Numbers**: SH1-xxxx
- **Software Version Numbers**: 1.6.0

### RF Features Tested

- **Radio Supported**: 802.11a/b/g/n

### QoS Features Supported / Tested

- **WMM**

### Powersave Features Tested

- **U-APSD**

### Encryption Supported

- **WPA2-PSK, PEAP-MSCHAPv2**

### Encryption Tested

- **WPA2-PSK, PEAP-MSCHAPv2**

### 802.11h Supported

- **Yes**

### Key Caching Support for Optimized Roaming

- **OKC and PMK**

### Voice Specific Features

- **Protocols Supported**: SIP-UDP, SIP-TCP, SIP-TLS
- **Control Traffic Pattern**: Handset to Server and vice versa
- **Voice Traffic Pattern**: Peer-to-peer (between handsets)
- **# of Calls per AP Tested**: 12 calls (not AP-capacity limited)

---

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution
**ArubaEdge Solution Qualification**

**Qualification Objective**
Validate the interoperability of the Ascom Myco with the Aruba’s wireless LAN infrastructure (version 6.4.2.5).

**Network Topology**

Software and hardware versions:
- Aruba 3400 controller v 6.4.2.5
- AP103, 115, 135, 205 and 225
- IP-PBX/SIP server
- Innovaphone IP6000 version 10 SR8
- Radius Server: FreeRadius
Settings on the Aruba WLAN

Enable SNMP v2 on the Aruba Mobility Controller, and configure the community string as follows:

The following Aruba Mobility Controller configuration settings are recommended for use with Ascom Myco handsets:

- RF Recommended Settings for Ascom
  - Beacon Interval: 100ms
  - DTIM Period: 5
  - WMM/ U-APSD Enabled
  - 802.11d Regulatory Domain: Country specific

- Encryption and Authentication
  - The handset and the WLAN infrastructure support and were tested with WPA/WPA2 enterprise and PSK. Please refer the Aruba configuration guide for additional information on how the SSIDs and encryption/authentication methods should be configured.

- Adaptive Radio Management
  - Enable ARM, voice aware scanning, WMM / UAPSD, and band steering.

- User Roles and Policies
  - The Ascom phones support SIP. So enable the voice ACL or the SIP ACLs

Ascom Settings

The following Ascom Myco Handset configuration settings are recommended for use with Aruba Mobility Controllers

Refer to Appendix A for additional details.
**Test Methodology**

**Summary Test Results**

The features and functions listed below were assessed during interoperability testing. The test results are presented in the right-most column.

**WLAN Controller Features**

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association, Open with No Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, WPA2-PSK, AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, PEAP-MSCHAPv2 Auth., AES Encryption</td>
<td>OK</td>
</tr>
<tr>
<td>Association, Multiple ESSIDs</td>
<td>OK</td>
</tr>
<tr>
<td>Beacon Interval and DTIM Period</td>
<td>OK</td>
</tr>
<tr>
<td>PMKSA Caching</td>
<td>OK</td>
</tr>
<tr>
<td>WPA2-Opportunistic/Proactive Key Caching</td>
<td>OK</td>
</tr>
<tr>
<td>WMM Prioritization</td>
<td>OK</td>
</tr>
<tr>
<td>Active Mode (load test)</td>
<td>OK</td>
</tr>
<tr>
<td>802.11 Power-Save Mode</td>
<td>OK</td>
</tr>
<tr>
<td>802.11e U-APSD</td>
<td>OK</td>
</tr>
<tr>
<td>802.11e U-APSD (load test)</td>
<td>OK</td>
</tr>
</tbody>
</table>
### Roaming

<table>
<thead>
<tr>
<th>High Level Functionality</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roaming, Open with No Encryption</td>
<td>OK (Avg roaming time 16ms) *</td>
</tr>
<tr>
<td>Roaming, WPA2-PSK, AES Encryption</td>
<td>OK (Avg roaming time 44ms) *</td>
</tr>
<tr>
<td>Roaming, PEAP-MSCHAPv2 Auth, AES Encryption</td>
<td>OK (Avg roaming time 51ms) <em>/</em>*</td>
</tr>
</tbody>
</table>

* ) Stated roaming times were measured using 802.11a/n/ac AP-225. Refer to Appendix B for detailed test records.

**) Results observed with Opportunistic Key Caching enabled.
**Know Limitations**

- Note that AP-205/214/215/224/225/275 only supports DTIM 1. This will reduce the standby (idle) time slightly to approximately 36 hours.

- Ascom Myco does not handle 802.11k info correctly which affects the roaming negatively. It is therefore highly recommended to configure the Aruba system **not** to advertise the 802.11K capabilities for the Ascom Myco SSID.

**Conclusion**

The verification, including association, authentication, roaming, and load test produced very good results overall. Roaming times were in general good with roaming times of around 40-50ms both when using WPA2-PSK/AES and PEAP-MSCHAPv2 (WPA2/AES).

Load testing showed that more than 12 Ascom Myco Handsets could maintain a call via a single Aruba access point when tested both in active and U-APSD modes. Note that 12 was the maximum number of devices tested and not the capacity limit.
Appendix 1
This section includes screenshots and explanations of basic settings required to use Ascom Myco Handsets with an Aruba 3400 Mobility Controller. Please note the security settings of each test case, as they were modified according to needs of the test cases.

The configuration file is found at the end of this appendix.

General settings (SSID, Radio and QoS)

Set DTIM Interval to 5 (for AP-204/205/214/215/224/225 only value 1 is supported). This value is recommended for maximum battery conservation without impacting call quality. Using a lower value will decrease the standby time slightly.
Ascom recommends disabling the lowest rates and recommends that 12mbits is the lowest basic rate.

Ensure that WMM and U-APSD are enabled. To match the default values in the Myco ensure to use DSCP 46 for Voice, 26 for video and 0 for best effort. It is also recommended that “Max Transmit Attempts” be set to 4.

**Note:** To further optimize performance it is recommended that 802.11b clients be disallowed from associating by setting 12Mbps as Basic Rates in the 802.11g configuration.
Set “Maximum Transmit Failures” to 25.

“High throughput enable” enables 802.11n capabilities that are supported in combination with Open encryption and WPA2-AES (PSK or Enterprise).
Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities.

**General guidelines when deploying Ascom Myco handsets in 802.11a/n/ac environments:**

1. **Enabling more than 8 channels will degrade roaming performance. Ascom recommends against going above this limit.**

2. **Using 40 MHz channels (or “channel-bonding”) will reduce the number of non-DFS* channels to two in ETSI regions (Europe). In FCC regions (North America), 40MHz is a more viable option because of the availability of additional non-DFS channels. The handset can co-exist with 40MHz stations in the same ESS.**

3. **Ascom do support and can coexist in 80MHz channel bonding environments. The recommendations is however to avoid 80Mhz channel bonding as it severely reduces the number of available non overlapping channels.**

4. **Make sure that all non-DFS channel are taken before resorting to DFS channels. The handset can cope in mixed non-DFS and DFS environments; however, due to “unpredictability” introduced by radar detection protocols, voice quality may become distorted and roaming delayed. Hence Ascom recommends if possible avoiding the use of DFS channels in VoWIFI deployments.**

*) Dynamic Frequency Selection (radar detection)
Ascom recommends a Beacon Interval of 100ms and advertising 802.11d/h capabilities. For 802.11b/g/n use only channels 1, 6 and 11. For 802.11a/n/ac, use channels in accordance with Aruba’s guidelines and in compliance with local regulations.

Encryption and Authentication Settings

WPA2-PSK. Set the security profile to WPA2-PSK, AES encryption.
Enterprise/.1X authentication.

Step 1: When configuring the authentication mode using a Radius server, the IP address and the secret must correspond to the IP address and the credential used by the Radius server. The RADIUS server should be added to a Server Group.

Step 2: Create an 802.1X Authentication Profile.
Step 3: Choose the 802.1X Authentication profile created in previous step and configure the Authentication Server group.

Choose configured AAA Profile and set WPA2/AES as the security mode.

See Appendix B for the controller configuration used for the certification process.
Ascom Myco Setting Summary

- Select Network to be active (In example “ArubaIntop” (created in step below)
- Select frequency band according to system setup (here 5GHz)
Pre-Shared key authentication

Network settings for WPA2-PSK
Authentication with dot1X (EAP/PEAP-MSCHAPv2)

802.1X Authentication requires a root certificate to be uploaded to the device by “right clicking” -> Manage Certificates.

Upload the required root CA under Trust list.
Network settings for .1X authentication (PEAP-MSCHAPv2)

- Select security mode PEAP-MSCHAPv2.
- Enter User identity and password.
- Select your trusted certificate uploaded to the device in previous step.
APPENDIX B

Test Summary

<table>
<thead>
<tr>
<th>Description</th>
<th>Runs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tests passed</td>
<td>18</td>
</tr>
<tr>
<td>Tests Not Run</td>
<td>1</td>
</tr>
<tr>
<td>Tests fail</td>
<td>0</td>
</tr>
<tr>
<td>Test NA</td>
<td>0</td>
</tr>
<tr>
<td>Total Number of Tests</td>
<td>19</td>
</tr>
</tbody>
</table>
Aruba Test Configuration File

version 6.4
enable secret *7d3998e20126db68084797bcc038534bffc2ced01c24555806*
hostname "Aruba3400"
clock timezone PST -8
location "Building1.floor1"
controller config 720
ip NAT pool dynamic-srcnat 0.0.0.0 0.0.0.0
ip access-list eth validuserethacl
  permit any
  !
  netservice svc-pcoip2-tcp tcp 4172
  netservice svc-snmp-trap udp 162
  netservice svc-netbios-dgm udp 138
  netservice svc-citrix tcp 2598
  netservice svc-smb-tcp tcp 445
  netservice svc-ike udp 500
  netservice svc-l2tp udp 1701
  netservice svc-syslog udp 514
  netservice svc-dhcp udp 67 68 alg dhcp
  netservice svc-https tcp 443
  netservice svc-ica tcp 1494
  netservice svc-pptp tcp 1723
  netservice svc-telnet tcp 23
  netservice svc-https tcp 88
  netservice svc-scocp tcp 2000 alg scocp
  netservice svc-sec-papi udp 8209
  netservice svc-web tcp list "80 443"*
  netservice svc-tftp udp 69 alg tftp
  netservice svc-kerberos udp 88
  netservice svc-sip-tcp tcp 5060
  netservice svc-netbios-ssn tcp 139
  netservice svc-pcoip-udp udp 50002
  netservice svc-pcoip-tcp tcp 50002
  netservice svc-pop3 tcp 110
  netservice svc-adp udp 8200
  netservice svc-cfgm-tcp tcp 8211
  netservice svc-noe udp 32512 32765 alg noe
  netservice svc-ftp udp 8888
  netservice svc-lpd-tcp tcp 631
  netservice svc-msrpc-tcp tcp 135 139
  netservice svc-rtsp tcp 554 alg rtsp
  netservice svc-dns udp 53 alg dns
  netservice vnc tcp 5900 5905
  netservice svc-vocera udp 5002 alg vocera
  netservice svc-h323-tcp tcp 1720
  netservice svc-h323-udp udp 1718 1719
  netservice svc-http tcp 80
  netservice svc-nterm tcp 1026 1028
  netservice svc-sip-udp udp 5060
  netservice svc-ftp tcp 8888
  netservice svc-nat udp 5000
  netservice svc-nat udp 5000
  netservice svc-nat udp 5000
  netservice svc-nat udp 5000
  netservice svc-sip-udp udp 8211
  netservice svc-ftp tcp 21 alg ftp
  netservice svc-nat udp 4500
  netservice svc-svp 119 alg svp
  netservice svc-microsoft-ds tcp 445
  netservice svc-gre 47
  netservice svc-smt tcp tcp 25
  netservice svc-smb-udp udp 445
  netservice svc-sips tcp 5061 alg sips
  netservice svc-netbios-ns udp 137
  netservice svc-esp 50
  netservice svc-cups tcp 515
  netservice svc-pcoip2-udp udp 4172
  netservice svc-bootp udp 67 69
netservice svc-snmp udp 161
netservice svc-v6-dhcp udp 546 547
netservice svc-icmp 1
netservice svc-ltp udp 123
netservice svc-msrpc-udp udp 135 139
netservice svc-ssh tcp 22
netservice svc-http-proxy1 tcp 3128
netservice svc-v6-icmp 58
netservice svc-lpd-udp udp 631
netservice svc-vmware-rdp tcp 3389
netdestination6 ipv6-reserved-range
inver
network 2000::/3
!
etexthdr default
!
time-range night-hours periodic
weekday 18:01 to 23:59
weekday 00:00 to 07:59
!
time-range weekend periodic
weekend 00:00 to 23:59
!
time-range working-hours periodic
weekday 08:00 to 18:00
!
ip access-list session allow-diskservices
any any svc-netbios-dgm permit
any any svc-netbios-ssn permit
any any svc-microsoft-ds permit
any any svc-netbios-ns permit
!
ip access-list session control
any any svc-papi permit
any any svc-sec-papi permit
user any udp 68 deny
any any svc-icmp permit
any any svc-dns permit
any any svc-ftp permit
tos 46 dot1p-priority 6
tos 46 dot1p-priority 6
tos 46 dot1p-priority 6
!
ip access-list session v6-icmp-acl
!
ip access-list session apprf-ascom-sacl
!
ip access-list session validuser
network 169.254.0.0 255.255.0.0 any any deny
network 127.0.0.0 255.0.0.0 any any deny
network 224.0.0.0 240.0.0.0 any any deny
host 255.255.255.255 any any deny
network 240.0.0.0 240.0.0.0 any any deny
any any permit
ipv6 host fe80:: any any deny
ipv6 network fc00::/7 any any permit
ipv6 network fe80::/64 any any permit
ipv6 alias ipv6-reserved-range any any deny
ipv6 any any permit
!
ip access-list session vocera-acl
any any svc-vocera permit queue high
!
ip access-list session v6-https-acl
!
ip access-list session vmware-acl
any any svc-vmware-rdp permit tos 46 dot1p-priority 6
any any svc-pcoip-tcp permit tos 46 dot1p-priority 6
any any svc-pcoip-udp permit tos 46 dot1p-priority 6

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution
any any svc-pcoip2-tcp  permit tos 46 dot1p-priority 6
going any any svc-pcoip2-udp  permit tos 46 dot1p-priority 6
!
ip access-list session apprf-default-vpn-role-sacl
!
ip access-list session v6-control
  ipv6 any any svc-papi  permit
  ipv6 any any svc-sec-papi  permit
  ipv6 user any udp 547 deny
  ipv6 any any svc-v6-icmp  permit
  ipv6 any any svc-dns  permit
  ipv6 any any svc-cfgm-tcp  permit
  ipv6 any any svc-adp  permit
  ipv6 any any svc-tftp  permit
  ipv6 any any svc-dhcp  permit
  ipv6 any any svc-natt  permit
!
ip access-list session icmp-acl
  any any svc-icmp  permit
!
ip access-list session apprf-authenticated-sacl
!
ip access-list session apprf-stateful-dot1x-sacl
!
ip access-list session captiveportal
  user alias controller svc-https dst-nat 8081
  user any svc-http dst-nat 8080
  user any svc-https dst-nat 8081
  user any svc-http-proxy1 dst-nat 8088
  user any svc-http-proxy2 dst-nat 8088
  user any svc-http-proxy3 dst-nat 8088
!
ip access-list session v6-dhcp-acl
!
ip access-list session allowall
  any any permit
!
ip access-list session v6-dns-acl
!
ip access-list session apprf-voice-sacl
!
ip access-list session lync-acl
  any any svc-sips permit queue high
!
ip access-list session test
!
ip access-list session sip-acl
  any any svc-sip-udp permit queue high
  any any svc-sip-tcp permit queue high
!
ip access-list session https-acl
  any any svc-https permit
!
ip access-list session citrix-acl
  any any svc-citrix permit tos 46 dot1p-priority 6
  any any svc-ica permit tos 46 dot1p-priority 6
!
ip access-list session dns-acl
  any any svc-dns permit
!
ip access-list session ascom
  any any permit
!
ip access-list session ra-guard
  ipv6 user any icmpv6 rtr-adv deny
!
ip access-list session allow-printservices
  any any svc-cups permit
  any any svc-lpd-tcp permit
  any any svc-lpd-udp permit

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution 25
ip access-list session logon-control
    user any udp 68 deny
    any any svc-icmp permit
    any any svc-dns permit
    any any svc-dhcp permit
    any any svc-natt permit
    any network 169.254.0.0 255.255.0.0 any deny
    any network 240.0.0.0 240.0.0.0 any deny
    ip access-list session vpilogon
    user any svc-ike permit
    user any svc-esp permit
    any any svc-l2tp permit
    any any svc-pptp permit
    any any svc-gre permit
ip access-list session srcnat
    user any src-nat
ip access-list session skinny-acl
    any any svc-sccp permit queue high
ip access-list session tftp-acl
    any any svc-tftp permit
ip access-list session v6-allowall
ip access-list session apprf-cpbase-sacl
ip access-list session cplgout
    user alias controller svc-https dst-nat 8081
ip access-list session apprf-default-via-role-sacl
ip access-list session dhcp-acl
    any any svc-dhcp permit
ip access-list session http-acl
    any any svc-http permit
ip access-list session v6-http-acl
ip access-list session captiveportal6
    ipv6 user alias controller6 svc-https captive
    ipv6 user any svc-https captive
    ipv6 user any svc-http captive
    ipv6 user any svc-http-proxy1 captive
    ipv6 user any svc-http-proxy2 captive
    ipv6 user any svc-http-proxy3 captive
ip access-list session apprf-guest-sacl
ip access-list session ap-uplink-acl
    any udp 68 permit
    any any svc-icmp permit
    any host 224.0.0.251 udp 5353 permit
ip access-list session ap-acl
    any any svc-gre permit
    any any svc-syslog permit
    any user svc-snmp permit
    user any svc-http permit
    user any svc-http-accl permit
    user any svc-mrpc-tcp permit
    user any svc-smtp-tcp permit
    user any svc-snmp-trap permit
    user any svc-ntp permit
    user alias controller svc-ftp permit
ip access-list session svp-acl
  any any svc-svp permit queue high
user host 224.0.1.116 any permit
!
ip access-list session noe-acl
  any any svc-noe permit queue high
!
ip access-list session global-sacl
!
ip access-list session v6-ap-acl
ipv6 any any svc-gre permit
ipv6 any any svc-syslog permit
ipv6 any user svc-snmp permit
ipv6 any user svc-snmp-trap permit
ipv6 user any svc-ntp permit
ipv6 user alias controller6 svc-ftp permit
!
ip access-list session h323-acl
  any any svc-h323-tcp permit queue high
  any any svc-h323-udp permit queue high
!
ip access-list session v6-logon-control
ipv6 any network fc00::/7 any permit
ipv6 any network fe80::/64 any permit
ipv6 any alias ipv6-reserved-range any deny
!
vpn-dialer default-dialer
  ike authentication PRE-SHARE e34b0dbf4989bec9a97af925e432d64558d0314b7ccf8655
!
user-role ap-role
  access-list session ra-guard
  access-list session control
  access-list session ap-acl
  access-list session v6-control
  access-list session v6-ap-acl
!
user-role denyall
!
user-role default-vpn-role
  access-list session global-sacl
  access-list session apprf-default-vpn-role-sacl
  access-list session ra-guard
  access-list session allowall
  access-list session v6-allowall
!
user-role cpbase
  access-list session global-sacl
  access-list session apprf-cpbase-sacl
!
user-role voice
  access-list session global-sacl
  access-list session apprf-voice-sacl
  access-list session ra-guard
  access-list session sip-acl
  access-list session noe-acl
  access-list session svp-acl
  access-list session vocera-acl
  access-list session skinny-acl
  access-list session h323-acl
  access-list session dhcp-acl
  access-list session ftp-acl
  access-list session dns-acl
  access-list session icmp-acl
!
user-role ascom
  access-list session global-sacl
  access-list session apprf-ascom-sacl
  access-list session ascom
!
user-role default-via-role
deploying ascom's myco vowifi handset with aruba networks' secure mobility solution
init-string AT+CGDCONT=1,"IP","zap.vivo.com.br"

dial-string ATD*99#

no spanning-tree

interface gigabitethernet 1/0
description "GE1/0"
    trusted
    trusted vlan 1-4094

interface gigabitethernet 1/1
description "GE1/1"
    trusted
    trusted vlan 1-4094

interface gigabitethernet 1/2
description "GE1/2"
    trusted
    trusted vlan 1-4094

interface gigabitethernet 1/3
description "GE1/3"
    trusted
    trusted vlan 1-4094

interface vlan 1
    ip address 192.168.0.13 255.255.255.0

    ip default-gateway 172.20.106.1
    ip default-gateway 192.168.0.50
    uplink disable

crypto isakmp policy 20
    encryption aes256

    crypto isakmp policy 10001

    crypto isakmp policy 10002
    encryption aes256
    authentication rsa-sig

    crypto isakmp policy 10003
    encryption aes256

    crypto isakmp policy 10004
    version v2
    encryption aes256
    authentication rsa-sig

    crypto isakmp policy 10005
    encryption aes256

    crypto isakmp policy 10006
    version v2
encryption aes128
authentication rsa-sig
!
crypto isakmp policy 10007
  version v2
  encryption aes128
!
crypto isakmp policy 10008
  version v2
  encryption aes128
  hash sha2-256-128
  group 19
  authentication ecdsa-256
  prf prf-hmac-sha256
!
crypto isakmp policy 10009
  version v2
  encryption aes256
  hash sha2-384-192
  group 20
  authentication ecdsa-384
  prf prf-hmac-sha384
!
crypto ipsec transform-set default-ha-transform esp-3des esp-sha-hmac
crypto ipsec transform-set default-boc-bm-transform esp-3des esp-sha-hmac
crypto ipsec transform-set default-rap-transform esp-aes256 esp-sha-hmac
crypto ipsec transform-set default-aes esp-aes256 esp-sha-hmac
crypto dynamic-map default-rap-ipsecmap 10001
  version v2
  set transform-set "default-gcm256" "default-gcm128" "default-rap-transform"
!
crypto dynamic-map default-dynamicmap 10000
  set transform-set "default-transform" "default-aes"
!
crypto map GLOBAL-IKEV2-MAP 10000 ipsec-isakmp dynamic default-rap-ipsecmap
crypto map GLOBAL-MAP 10000 ipsec-isakmp dynamic default-dynamicmap
crypto isakmp eap-passthrough eap-tls
crypto isakmp eap-passthrough eap-peap
crypto isakmp eap-passthrough eap-mschapv2

vpdn group l2tp
!

!
vpdn group pptp
!
tunneled-node-address 0.0.0.0

adp discovery enable
adp igmp-join enable
adp igmp-vlan 0

voice rtcp-inactivity disable
voice alg-based-cac enable
voice sip-midcall-req-timeout disable
ap ap-blacklist-time 3600
ap flush-r1-on-new-r0 disable

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution
no ssh mgmt-auth public-key
ssh mgmt-auth username/password
mgmt-user admin root 5436b5a101681372db26d314e974065944317cd3e1fe6a5534

no database synchronize
ip mobile domain default
!
!
airgroup mdns "enable"
!
airgroup dina "enable"
!
airgroup location-discovery "enable"
!
airgroup active-wireless-discovery "disable"
!
airgroupservice "airplay"
  id "_airplay._tcp"
  id "_raop._tcp"
  id "_apple-tv-v2._tcp"
  description "AirPlay"
!
airgroupservice "airprint"
  id "_ipp._tcp"
  id "_pdl-datasync._tcp"
  id "_printer._tcp"
  id "_scanner._tcp"
  id "_universal_sub_ipp._tcp"
  id "_universal_sub_ipps._tcp"
  id "_printer_sub_http._tcp"
  id "_http._tcp"
  id "_http-alt._tcp"
  id "_ipp-tls._tcp"
  id "_fax-ipp._tcp"
  id "_rious_print._tcp"
  id "_cups_sub_ipp._tcp"
  id "_cups_sub_fax-ipp._tcp"
  id "_ica-networking._tcp"
  id "_lp._tcp"
  id "_canon-binp1._tcp"
  id "_ipps._tcp"
  id "_ica-networking2._tcp"
  description "AirPrint"
!
airgroupservice "itunes"
  id "_home-sharing._tcp"
  id "_apple-mobdev._tcp"
  id "_daap._tcp"
  id "_daccp._tcp"
  description "iTunes"
!
airgroupservice "remotemgmt"
  id "_ssh._tcp"
  id "_sftp-ssh._tcp"
  id "_ftp._tcp"
  id "_telnet._tcp"
  id "_rfb._tcp"
  id "_net-assistant._tcp"
  description "Remote management"
!
airgroupservice "sharing"
  id "_odisk._tcp"
  id "_afpvoicetcp._tcp"
  id "_xgrid._tcp"
  description "Sharing"
airgroupservice "chat"
  id "_presence._tcp"
  description "Chat"

airgroupservice "googlecast"
  id "_googlecast._tcp"
  description "GoogleCast supported by Chromecast etc"

airgroupservice "DIAL"
  id "urn:dial-multiscreen-org:service:dial:1"
  id "urn:dial-multiscreen-org:device:dial:1"
  description "DIAL supported by Chromecast, FireTV, Roku etc"

airgroupservice "DLNA Media"
  id "urn:schemas-upnp-org:device:MediaServer:1"
  id "urn:schemas-upnp-org:device:MediaServer:2"
  id "urn:schemas-upnp-org:device:MediaServer:3"
  id "urn:schemas-upnp-org:device:MediaServer:4"
  id "urn:schemas-upnp-org:device:MediaRenderer:1"
  id "urn:schemas-upnp-org:device:MediaRenderer:2"
  id "urn:schemas-upnp-org:device:MediaRenderer:3"
  id "urn:schemas-upnp-org:device:MediaPlayer:1"
  description "Media"

airgroupservice "DLNA Print"
  id "urn:schemas-upnp-org:device:Printer:1"
  id "urn:schemas-upnp-org:service:PrintBasic:1"
  id "urn:schemas-upnp-org:service:PrintEnhanced:1"
  description "Print"

airgroupservice "allowall"
  description "Remaining-Services"

airgroup service "airplay" enable

airgroup service "airprint" enable

airgroup service "itunes" disable

airgroup service "remotemgmt" disable

airgroup service "sharing" disable

airgroup service "chat" disable

airgroup service "googlecast" disable

airgroup service "DIAL" enable

airgroup service "DLNA Media" disable

airgroup service "DLNA Print" disable

airgroup service "allowall" disable

ip igmp

ipv6 mld

no firewall attack-rate cp 1024
firewall enable ICE-STUN based firewall traversal
firewall attack-rate grat-arp 50 drop
ipv6 firewall ext-hdr-parse-len 100

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution
! firewall cp
! ip domain lookup
! country US
aaa authentication mac "default"
! aaa authentication dot1x "ArubaIntop-dot1x_prof"
! aaa authentication dot1x "ascom"
  machine-authentication enable
  machine-authentication machine-default-role "ascom"
  machine-authentication user-default-role "authenticated"
  reauthentication
  termination enable
  termination eap-type eap-peap
  termination inner-eap-type eap-mschapv2
! aaa authentication dot1x "default"
! aaa authentication dot1x "Freeradius"
  machine-authentication enable
  machine-authentication machine-default-role "ascom"
  machine-authentication user-default-role "authenticated"
! aaa authentication-server radius "Intop"
  host "192.168.0.2"
  key 27ee879db0798fec4b7e22f99247071c
! aaa server-group "ascom"
  auth-server Internal
! aaa server-group "default"
  auth-server Internal
  set role condition role value-of
! aaa server-group "intop"
  auth-server Intop
! aaa profile "ascom"
  initial-role "ascom"
  authentication-dot1x "ascom"
  dot1x-default-role "authenticated"
  dot1x-server-group "ascom"
! aaa profile "default"
  authentication-dot1x "ascom"
  dot1x-default-role "authenticated"
  dot1x-server-group "ascom"
! aaa profile "default-dot1x"
  initial-role "ascom"
  authentication-dot1x "Freeradius"
  dot1x-default-role "authenticated"
  dot1x-server-group "intop"
! aaa profile "default-dot1x-psk"
  initial-role "ascom"
  authentication-dot1x "default-psk"
  dot1x-default-role "authenticated"
! aaa authentication captive-portal "default"
! aaa authentication wispr "default"
! aaa authentication vpn "default"
! aaa authentication vpn "default-rap"
aaa authentication mgmt

! aaa authentication stateful-ntlm "default"

! aaa authentication stateful-kerberos "default"

! aaa authentication stateful-dot1x
  server-group "intop"

! aaa authentication wired

! web-server profile

! guest-access-email

! voice logging

! voice dialplan-profile "default"

! app lync traffic-control "default"

! voice real-time-config

! voice sip

! aaa password-policy mgmt

! control-plane-security
  no cpsec-enable

! ids wms-general-profile
  poll-retries 3

! ids wms-local-system-profile

! valid-network-oui-profile

! upgrade-profile

! license profile

! activate-service-whitelist

! file syncing profile

! ifmap cppm

! pan profile "default"

! pan active-profile

! ap system-profile "default"

! ap regulatory-domain-profile "default"
  country-code US
  valid-11g-channel 1
  valid-11g-channel 6
  valid-11g-channel 11
  valid-11a-channel 36
  valid-11a-channel 40
  valid-11a-channel 44
  valid-11a-channel 48
  valid-11a-channel 149
  valid-11a-channel 153
  valid-11a-channel 157
  valid-11a-channel 161
  valid-11a-channel 165
  valid-11g-40mhz-channel-pair 1-5
  valid-11g-40mhz-channel-pair 7-11
  valid-11a-40mhz-channel-pair 36-40
valid-11a-40mhz-channel-pair 44-48
valid-11a-40mhz-channel-pair 149-153
valid-11a-40mhz-channel-pair 157-161

! ap wired-ap-profile "default"
! ap enet-link-profile "default"
! ap mesh-ht-ssid-profile "default"
! ap lldp med-network-policy-profile "default"
! ap mesh-cluster-profile "default"
! ap lldp profile "default"
! ap mesh-radio-profile "default"
! ap wired-port-profile "default"
! ids general-profile "default"
! ids unauthorized-device-profile "default"
! ids profile "default"
! rf arm-profile "default"
    assignment disable
! rf arm-profile "disable"
    assignment disable
    no scanning
    no multi-band-scan
! rf optimization-profile "default"
! rf event-thresholds-profile "default"
! rf am-scan-profile "default"
! rf dot11a-radio-profile "ch 165"
    no very-high-throughput-enable
    channel 165
    tx-power 6
    arm-profile "disable"
! rf dot11a-radio-profile "ch 36"
    channel 36E
    tx-power 12
dot11h
    arm-profile "disable"
! rf dot11a-radio-profile "ch 40"
    no very-high-throughput-enable
    channel 40
    tx-power 12
dot11h
! rf dot11a-radio-profile "ch149"
    channel 149+
    tx-power 14
dot11h
! rf dot11a-radio-profile "ch157"
    channel 157+
    tx-power 12
dot11h
! rf dot11a-radio-profile "ch44"
    channel 44

Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution

35
wlan hotspot anqp-domain-name-profile "default"
!
wlan wmm-traffic-management-profile "Ascom"
  enable-shaping
!
wlan edca-parameters-profile station "default"
!
wlan edca-parameters-profile ap "default"
!
wlan dot11k-profile "default"
!
wlan ssid-profile "--NEW--"
  essid "ArubaIntop2"
  wmm-vo-dscp "56"
  wmm-vi-dscp "40"
  wmm-be-dscp "24"
  wmm-bk-dscp "8"
!
wlan ssid-profile "ArubaIntop1x"
  essid "ArubaIntop1x"
  opmode wpa2-aes
  dtim-period 5
  g-basic-rates 12
  g-tx-rates 12 18 24 36 48 54
  max-retries 4
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "26"
  wmm-bk-dscp "8"
  max-tx-fail 25
!
wlan ssid-profile "ArubaIntopOpen"
  essid "ArubaIntopOpen"
  dtim-period 5
  g-basic-rates 12
  g-tx-rates 5 6 12 18 24 36 48 54
  max-retries 4
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "26"
  wmm-bk-dscp "8"
  max-tx-fail 25
  edca-parameters-profile station "default"
  edca-parameters-profile ap "default"
!
wlan ssid-profile "default"
  essid "ArubaIntop"
  opmode wpa2-psk-aes
  dtim-period 5
  g-basic-rates 8
  g-tx-rates 12 18 24 36 48 54
  max-retries 4
  wmm
  wmm-vo-dscp "46"
  wmm-vi-dscp "40"
  wmm-be-dscp "26"
  wmm-bk-dscp "8"
  wepkey1 78d16bcbee9125fc17b129c2f5d8bdffda804605e9e4053
  wpa-passphrase 947419354b5e2ecd0843516e728a6c2e86ac8b86c03c08c
  max-tx-fail 25
  edca-parameters-profile station "default"
  edca-parameters-profile ap "default"
!
wlan ssid-profile "test"
  opmode wpa2-psk-aes
  wmm-vo-dscp "56"
  wmm-vi-dscp "40"
  wmm-be-dscp "24"
Deploying Ascom’s Myco VoWi-Fi Handset with Aruba Networks’ Secure Mobility Solution
dot11a-radio-profile "ch 36"
dot11g-radio-profile "channel-1"
!
airgroup cppm-server aaa
!
logging level warnings security subcat ids
logging level warnings security subcat ids-ap

snmp-server enable trap
snmp-server trap source 0.0.0.0
snmp-server trap disable wlsxAdhocNetwork
snmp-server trap disable wlsxAdhocNetworkBridgeDetectedAP
snmp-server trap disable wlsxAdhocNetworkBridgeDetectedSta
snmp-server trap disable wlsxAdhocUsingValidSSID
snmp-server trap disable wlsxAuthMaxAclEntries
snmp-server trap disable wlsxAuthMaxBWContracts
snmp-server trap disable wlsxAuthMaxUserEntries
snmp-server trap disable wlsxAuthServerIsUp
snmp-server trap disable wlsxAuthServerReqTimedOut
snmp-server trap disable wlsxChannelChanged
snmp-server trap disable wlsxCoverageHoleDetected
snmp-server trap disable wlsxDBCommunicationFailure
snmp-server trap disable wlsxDisconnectStationAttack
snmp-server trap disable wlsxESIServerDown
snmp-server trap disable wlsxESIServerUp
snmp-server trap disable wlsxFanFailure
snmp-server trap disable wlsxFan Tray Inserted
snmp-server trap disable wlsxFan Tray Removed
snmp-server trap disable wlsxGBIC Inserted
snmp-server trap disable wlsxGBIC Removed
snmp-server trap disable wlsxLicense Expiry
snmp-server trap disable wlsxLow Memory
snmp-server trap disable wlsxLow On Flash Space
snmp-server trap disable wlsxOutOfRangeTemperature
snmp-server trap disable wlsxOutOfRangeVoltage
snmp-server trap disable wlsxPowerSupplyFailure
snmp-server trap disable wlsxPowerSupplyMissing
snmp-server trap disable wlsxProcessDied
snmp-server trap disable wlsxProcessExceedsMemoryLimits
snmp-server trap disable wlsxSC Inserted
snmp-server trap disable wlsxSignatureMatch
snmp-server trap disable wlsxSta UnAssociatedFromUnsecureAP
snmp-server trap disable wlsxSta UnAssociatedFromSta
snmp-server trap disable wlsxStation Added To BlackList
snmp-server trap disable wlsxStation Removed From BlackList
snmp-server trap disable wlsxSwitchIP Changed
snmp-server trap disable wlsxSwitchRole Change
snmp-server trap disable wlsxUserAuthentication Failed
snmp-server trap disable wlsxUserEntry Authenticated
snmp-server trap disable wlsxUserEntry Changed
snmp-server trap disable wlsxUserEntry Created
snmp-server trap disable wlsxUserEntry De Authenticated
snmp-server trap disable wlsxUserEntry Deleted
snmp-server trap disable wlsxVrrpState Change
firewall-visibility

process monitor log
end