

**AirDefense Services Platform**  
**Zero Touch**  
**WLAN Infrastructure**  
**Deployment Instructions**





## ***Contents***

1.0 Summary .....	1
2.0 Deployment Requirements .....	2
3.0 Support and Sales .....	9



# 1 Summary

Zero touch configuration enables taking Motorola wireless LAN infrastructure products directly out of the box and simply plugging it into the network for operational use. By coordination with the management platform the infrastructure is able to automatically receive the configuration needed to allow it to be used for operational needs. This process eliminates the need for any manual configuration or staging greatly simplifying deployments of WLAN infrastructure for client access and sensors. Zero touch works through a simple 3 step process.

1. Infrastructure boots and sends a trap to ADSP to notify it's a new device on the network.
2. ADSP receives the trap, recognizing it is from an unknown device will perform a single device discovery to import the newly added device into the management platform
3. Once placed in the tree hierarchy appropriately the system will automatically push a configuration template to the device setting the appropriate configuration for this device. The device is now fully up and operational without any manual staging or configuration.

## Document Conventions

The following graphical alerts are used in this document to indicate notable situations:



**NOTE** This symbol indicates something of special interest or importance to the reader. Failure to read the note will not result in physical harm to the reader, equipment or data.



**CAUTION** This symbol indicates that if this information is ignored, the possibility of data or material damage may occur.



**WARNING!** This symbol indicates that if this information is ignored the possibility that serious personal injury may occur.

## 2 Deployment Requirements

The following deployment requirements must be met:

- ADSP 8.1.2 or Newer
  - WLAN infrastructure management licenses are required to enable this feature
- Motorola WLAN Infrastructure running 5.1 or newer
- Network with DHCP enabled
- DNS entry for the host AirDefense1 in the domain of the DHCP scope the WLAN device will be initially attached to
- This solution does support DNS devolution
- Network which is able to route traffic and permit the following flows:
  - SNMP traps (UDP port 162) traffic from the infrastructure to the ADSP appliance
  - SNMP query traffic (UDP port 161) between ADSP and the infrastructure
  - SSH application traffic between the ADSP appliance and the infrastructure
  - SFTP or FTP traffic between the device and the Relay server (Could be same system as the ADSP appliance)
  - SFTP or FTP traffic between ADSP and the external relay server when one is used.

### Setup Prerequisites

Follow these steps to prepare deployment:

1. Enable SNMP Trap reception on the ADSP appliance:
  - a. From the ADSPadmin utility on the appliance console select C for Config then SNMP for Enable/Disable SNMP trap reception.
  - b. Select **E** for enable and save changes as shown below:

```
SNMP currently disabled

(E) Enable SNMP

(Q) to quit (return to previous menu)  -> █

Save the SNMP state as shown above? (yes/no): yes

iptables: Flushing firewall rules:          [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Uploading modules:                [ OK ]
iptables: Applying firewall rules:          [ OK ]
iptables: Loading additional modules: ip_conntrack_tftp [ OK ]

(Press <CR> to return to previous menu)
```

2. Verify Discovery SNMP Parameters:
  - a. In the appliance GUI, go to **Configuration** tab > **Appliance Platform** > **Communication Settings**.
  - b. Click on the **Unplaced Devices** folder.
    - ✓ **NOTE** When performing a discovery based on receiving a SNMP trap from a device, the system will use credentials based on the profile(s) set on the **Unplaced Devices** folder. The **Unplaced Devices** folder must have the default credentials for the device being deployed for the discovery to work successfully.
  - c. Uncheck default profiles for device types which will not be placed on your network.

*For example, for deployments of just WiNG 5.1 devices, you would uncheck all default profiles but the Motorola WiNG 5.x Default.*

*If more than one device type is being deployed, setting the unplaced device folder to inherit rather than override is sufficient.*
3. Verify Device Communication Settings:
  - a. In the appliance GUI, go to **Configuration** tab > **Appliance Platform** > **Communication Settings**.
  - b. Click on the top level of the tree to show currently applied profiles.
  - c. Uncheck default profiles for device types which will not be placed on your network.

*For example, for deployments of just WiNG 5.1 devices, you would uncheck all default profiles but the Motorola WiNG 5.x Default.*

    - ✓ **NOTE** Leaving all profiles checked will not prevent the zero touch feature from working but it will slow down the process.

*WHAT IS NEEDED?*

- d. Add a new profile which uses the non default production credentials that the infrastructure will have after completion of the zero touch configuration.

**Communication Settings Profile**

Profile Name:

SNMP Console HTTP

Enable Console settings

User:

Password:   Display Passwords

Enable Password:

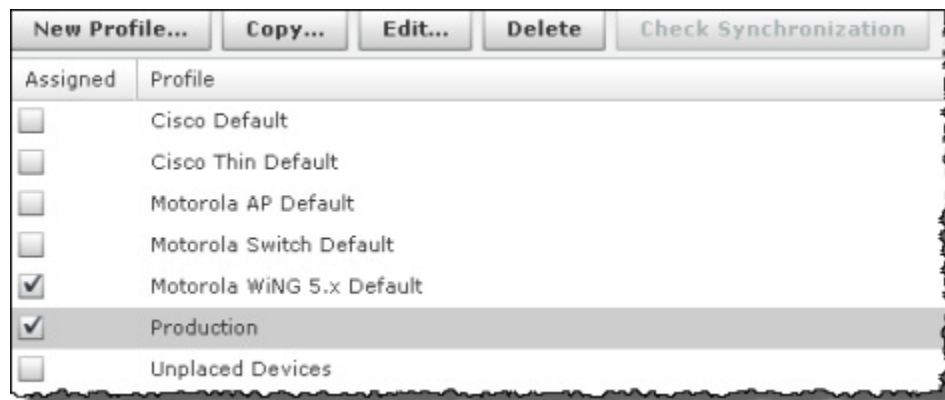
Protocol:

Port:

Save Cancel



Once complete, profile assignment should look like below:



Assigned	Profile
<input type="checkbox"/>	Cisco Default
<input type="checkbox"/>	Cisco Thin Default
<input type="checkbox"/>	Motorola AP Default
<input type="checkbox"/>	Motorola Switch Default
<input checked="" type="checkbox"/>	Motorola WiNG 5.x Default
<input checked="" type="checkbox"/>	Production
<input type="checkbox"/>	Unplaced Devices

4. Setup network device configuration action:
  - a. The system must be enabled to allow configuration push to the new infrastructure devices. To set this up, go to **Configuration** tab > **Appliance Platform** > **Polling**.
  - b. Enable the following settings:
    - Automatically Correct Configuration Compliance Violations
    - Device Configuration Management

- Template Based Configuration Management

**Copy settings to all appliances**

Enable automatic status polling  
Frequency:

Enable automatic data collection  
Frequency:

Automatically correct configuration compliance violations

---

Enable ACL

Enable port suppression

Enable background switch port scanning

Enable Device Configuration Management

Audit Only

Template Based Configuration Management

5. Set up Relay Server:
  - a. Configure the relay server for use with configuration management. The relay server setup is not specific to the zero touch feature, instructions for setup can be found in **Menu -> Help -> Search for Relay**.
6. Configuration non default device credentials:
  - a. Some infrastructure devices require changing the administrator password at first login. The ADSP system must be setup with the credentials to use for configuring the device. The credentials can be set by going to **Configuration tab > Infrastructure Management > Device Access**.
  - b. Enable Configuration.

- c. Add an **admin** user with password. Make sure this password is different than the default since most devices will reject resetting the password to the default value.

Enable configuration **Copy settings to all appliances**

Encrypt Passwords and Keys on Flash

Enable Password:   Display Passwords

Username	Password
admin	*****

✓ **NOTE** For devices which require password change at first login, this is the password the system shall use when rotating the password. Also, it should match the console and the http password for the "production" communication profile.

- d. Specify the interfaces to be used. If using SNMP access, specify read and write community passwords.

Enable configuration **Copy settings to all appliances**

Telnet access enabled

SSH access enabled

HTTP access enabled

HTTPS access enabled

SNMP access enabled

Read Community:   Display Passwords

Write Community:

Trap Community:

Trap Destination:

- e. Click **Apply** to save changes.
7. Set up CLI configuration push:
    - a. Set up a CLI template to push the configuration to the device. This template can include just a few lines of code to set the device as a sensor or can include a complete configuration to set and configure all parameters on the device. To create a configuration template go to **Configuration > Infrastructure Management > CLI Configuration** and select the specific device type of interest.
      - ✓ **NOTE** Partial configuration updates should only be done on the running configuration. If the template contains partial configuration, please select the **Do not reboot device, instead write updates to running configuration** option. This is to ensure that the device does not store a partial configuration as the start-up configuration.
    - b. CLI expansions can also be used but the corresponding profiles (WLAN, Radio, Channel, Device Access, RF Domain, ...) need to be configured as well.
      - ✓ **NOTE** Make sure that the configuration template and related profiles (WLAN, Radio, Channel, Device Access, RF Domain, ...) are well tested and validated prior to using them in zero config. A poorly written CLI template has the potential to isolate the device from the network.
      - ✓ **NOTE** After initial discovery, the process to fully import the device and place in a compliant state may take up to 2 data collection cycles for this to happen.

## 3 Support and Sales

### ***Motorola Solutions Support Center***

If you have a problem with your equipment, contact support for your region. Support and issue resolution is provided for products under warranty or that are covered by a Motorola Solutions Services agreement. Contact information and web self-service is available by visiting <http://supportcentral.motorola.com/>.

When contacting support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Motorola Solutions responds to calls by email or telephone within the time limits set forth in support agreements. If you purchased your business product from a Motorola Solutions business partner, contact that business partner for support.

### ***Customer Support Website***

Motorola Solutions Support Website, located at <http://supportcentral.motorola.com/> provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

### ***Manuals***

<http://supportcentral.motorola.com/support/product/manuals.do>



Motorola Solutions, Inc.  
1301 E. Algonquin Rd.  
Schaumburg, IL 60196-1078, U.S.A.  
<http://www.motorolasolutions.com>

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.  
© 2012 Motorola Solutions, Inc. All Rights Reserved.

