Zero Touch Wireless Deployment with Juniper Networks EX Series Switches and Aerohive Access Points

Configuration Guide

June 2016

© 2016 Juniper Networks, Inc.

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Contents

What this Document Covers 4
Platforms Used for Testing 4
Juniper Networks EX Series ZTP Overview 4
Aerohive Device Onboarding in HiveManager 5
Topology 7
Setting Up ZTP Environment 7
DHCP Server Configuration 7
Using Juniper Networks Junos Space Network Director to Prepare ZTP Environment 7
EX Series Switch Port Configuration 11
ZTP in Action 12
EX Series Switch Auto-Registration with Network Director 13
Aerohive Auto-Provisioning in HiveManager 14
Conclusion 18
Appendix – Sample Configurations 19

© 2016 Juniper Networks, Inc.

What this Document Covers

The objective of this document is to demonstrate plug-and-play deployment of Juniper Networks® EX Series switches and Aerohive access points. We will be using the Zero-Touch Provisioning (ZTP) capabilities on the EX Series switches and auto-provisioning capabilities on Aerohive access points. We will also cover how to use Juniper Networks Junos Space Network Director to set up the ZTP environment.

Platforms Used for Testing

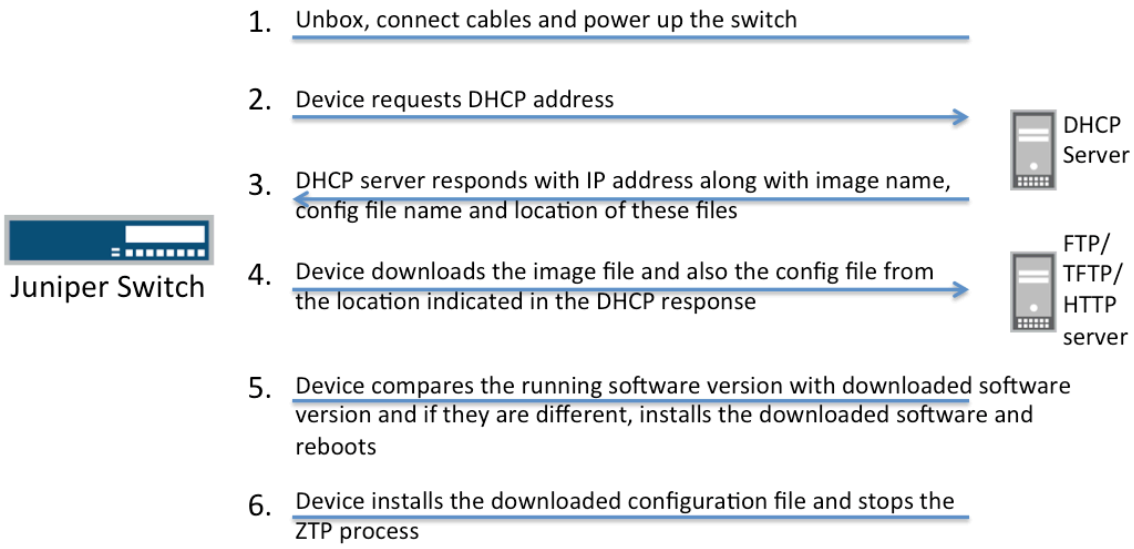
The following platforms are used in this demonstration.

- Juniper Networks EX4300 switch
- Aerohive AP230 access point
- Juniper Networks Junos Space Network Director 2.5
- CentOS DHCP server
- FileZilla FTP server

The capabilities demonstrated are available on all Juniper Networks switching platforms.

Juniper Networks EX Series ZTP Overview

ZTP allows automatic provisioning of new switches without manual intervention. When a switch is connected to the network and powered up with factory default configuration, the ZTP process on the switch downloads the appropriate software and also the configuration file for the device. The basic ZTP process will provide a standard configuration file based on the type of device. For example, all EX4300 switches in a particular branch office will get a particular Junos software version and a standard configuration file for EX4300 switches for that branch office. The following illustration shows the basic ZTP process.



At the completion of the ZTP process, the switch will have the correct Junos software and will also have a configuration file that is common for that platform in a site.

In this document, we will demonstrate how to address key requirements in an enterprise environment.

- Non-engineering staff should be able to handle basic maintenance tasks, such as:
  - Deploying new access switches in branch offices

© 2016 Juniper Networks, Inc.

  - Replacing access switches in branch offices
  - Deploying new Aerohive access points
  - Replacing Aerohive access points
- The only requirement from the onsite staff should be to cable the switch and the access points and power up the switch:
  - The new switch should have the ports automatically configured depending on the needs of the location.
  - The new switch should be automatically configured with a dynamic IP address.
  - Any new switch replacing a broken switch should automatically get the configuration necessary for the switch to perform its functions in that location.
- These switches should be functional after they are cabled and powered up without any CLI or GUI intervention.
- The ports on which Aerohive access points are connected should be preconfigured with required set up.
- At the end of the process, the newly added EX Series switch will automatically register on Network Director and show up in the Network Director GUI.
- The Aerohive access point will establish communication with HiveManager and will automatically get its configuration and firmware if auto-provisioning has been enabled.

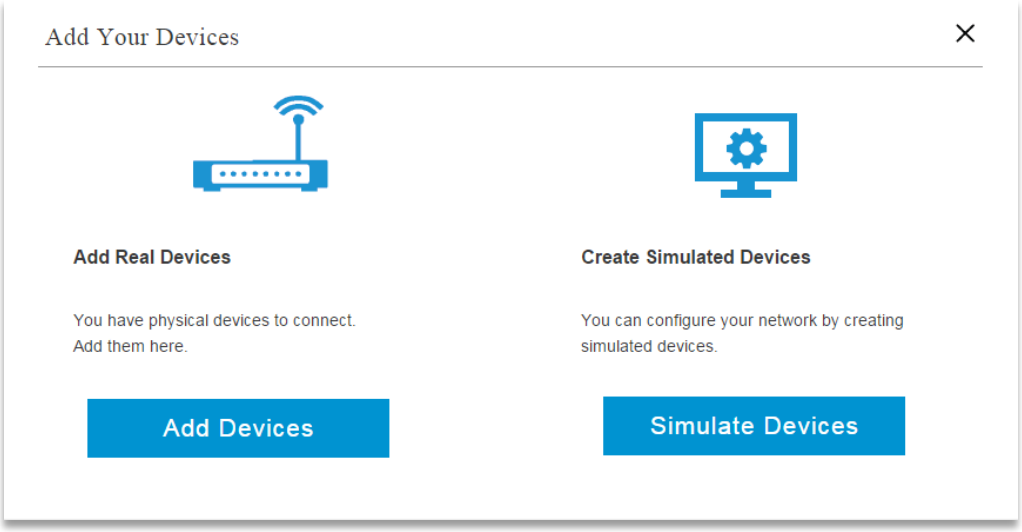
Aerohive Device Onboarding in HiveManager

Auto-provisioning allows administrators to quickly deploy Aerohive devices. With auto-provisioning, once an Aerohive device communicates with the HiveManager, the device will automatically receive the latest configuration and firmware. This significantly shortens the time and effort required to deploy an Aerohive WiFi solution.

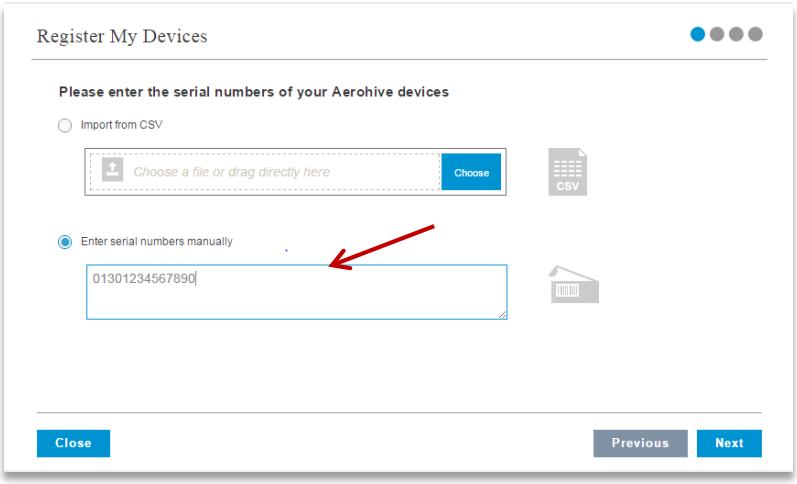
The first step is to onboard the devices.

1. Login to HiveManager NG and click the ⊕ **Menu Shortcut** icon

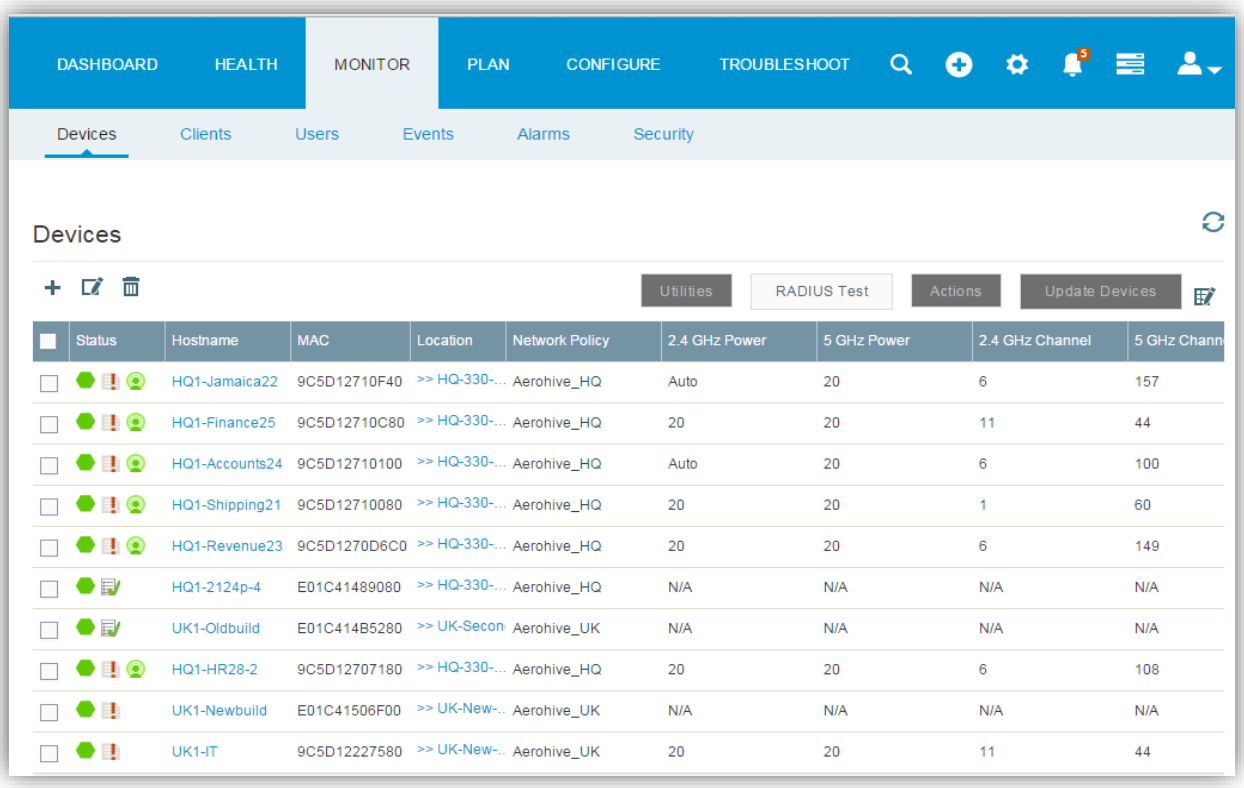
2. Select Onboard Devices from the drop-down menu
3. Click Add Real Devices



4. Enter the serial numbers or import the CSV file that you received.



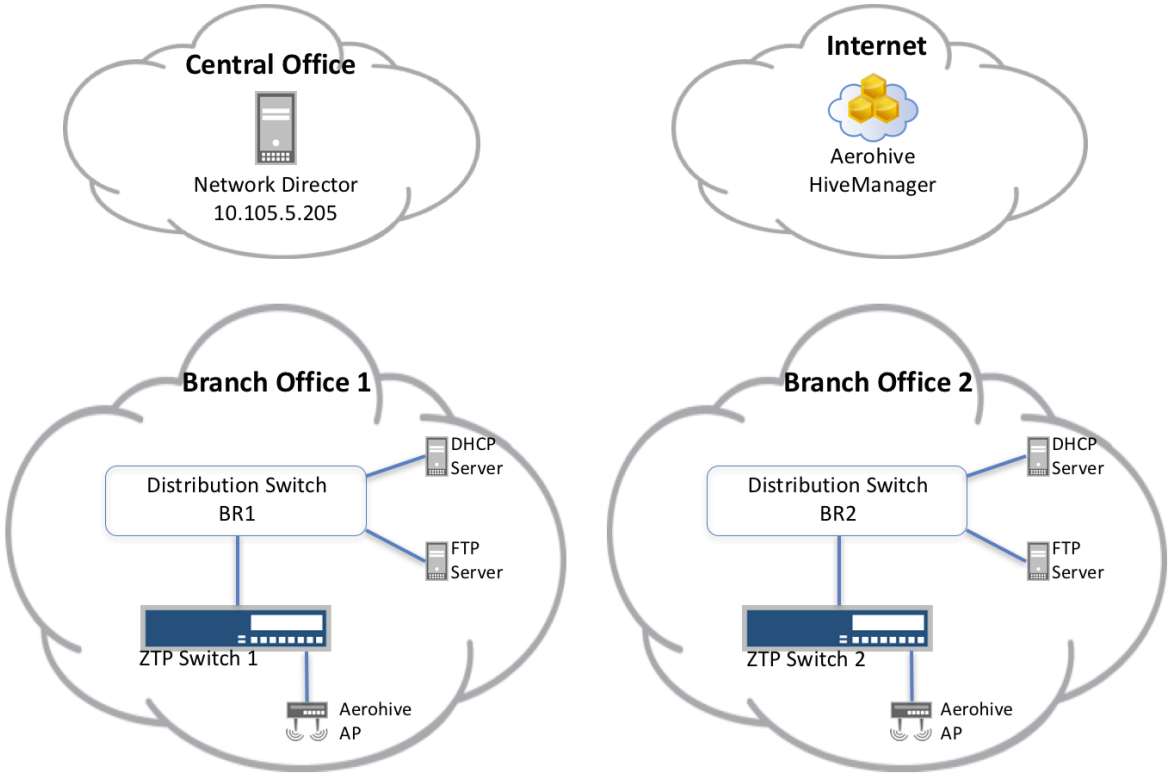
5. Click Next. Click Next. Click Close.
6. Devices will appear in the **Monitor** tab > **Devices** list with a green status icon. This indicates the devices have been successfully on-boarded. *Note: the process may take up to 15 minutes of HiveOS activity on the devices that have to be upgraded.*



Status	Hostname	MAC	Location	Network Policy	2.4 GHz Power	5 GHz Power	2.4 GHz Channel	5 GHz Chann
	HQ1-Jamaica22	9C5D12710F40	>> HQ-330-...	Aerohive_HQ	Auto	20	6	157
	HQ1-Finance25	9C5D12710C80	>> HQ-330-...	Aerohive_HQ	20	20	11	44
	HQ1-Accounts24	9C5D12710100	>> HQ-330-...	Aerohive_HQ	Auto	20	6	100
	HQ1-Shipping21	9C5D12710080	>> HQ-330-...	Aerohive_HQ	20	20	1	60
	HQ1-Revenue23	9C5D1270D6C0	>> HQ-330-...	Aerohive_HQ	20	20	6	149
	HQ1-2124p-4	E01C41489080	>> HQ-330-...	Aerohive_HQ	N/A	N/A	N/A	N/A
	UK1-Oldbuild	E01C414B5280	>> UK-Secon	Aerohive_UK	N/A	N/A	N/A	N/A
	HQ1-HR28-2	9C5D12707180	>> HQ-330-...	Aerohive_HQ	20	20	6	108
	UK1-Newbuild	E01C41506F00	>> UK-New-...	Aerohive_UK	N/A	N/A	N/A	N/A
	UK1-IT	9C5D12227580	>> UK-New-...	Aerohive_UK	20	20	11	44

© 2016 Juniper Networks, Inc.

Topology



Setting Up ZTP Environment

The network administrator must set up the environment to support the ZTP process, and this section provides an example of how to do that. Network administrators can manually prepare all tasks shown below; however, this example will show how network administrators can use Network Director to prepare the environment the ZTP environment.

DHCP Server Configuration

DHCP server should be configured to identify the type of device requesting a DHCP address (in this case the EX4300) and send back the following information along with the DHCP response.

- Software image file name
- Configuration file name
- File transfer mode
- Server IP address where these files are located

A sample DHCP configuration file is available at the end of this document. Network administrators can prepare this configuration manually, or they can use Network Director to generate this configuration. In this example, we will show how to use Network Director to populate the dhcpd.conf file.

Using Juniper Networks Junos Space Network Director to Prepare ZTP Environment

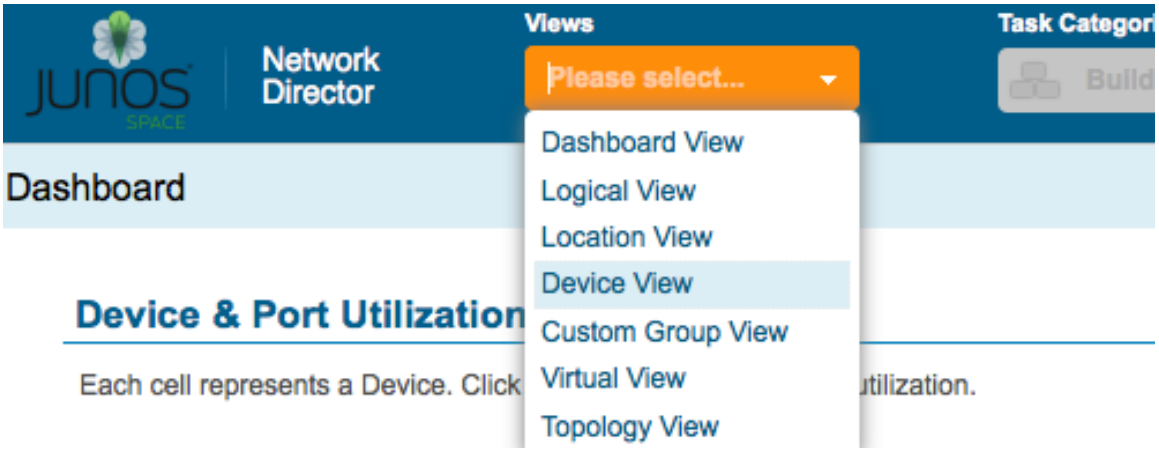
The ZTP environment can be set up either manually or through Network Director. If you would like to set up the ZTP environment manually, please refer to the sample configuration files provided in the Appendix.

This section will show how to use Network Director to setup the environment. Network Director can setup the following for ZTP:

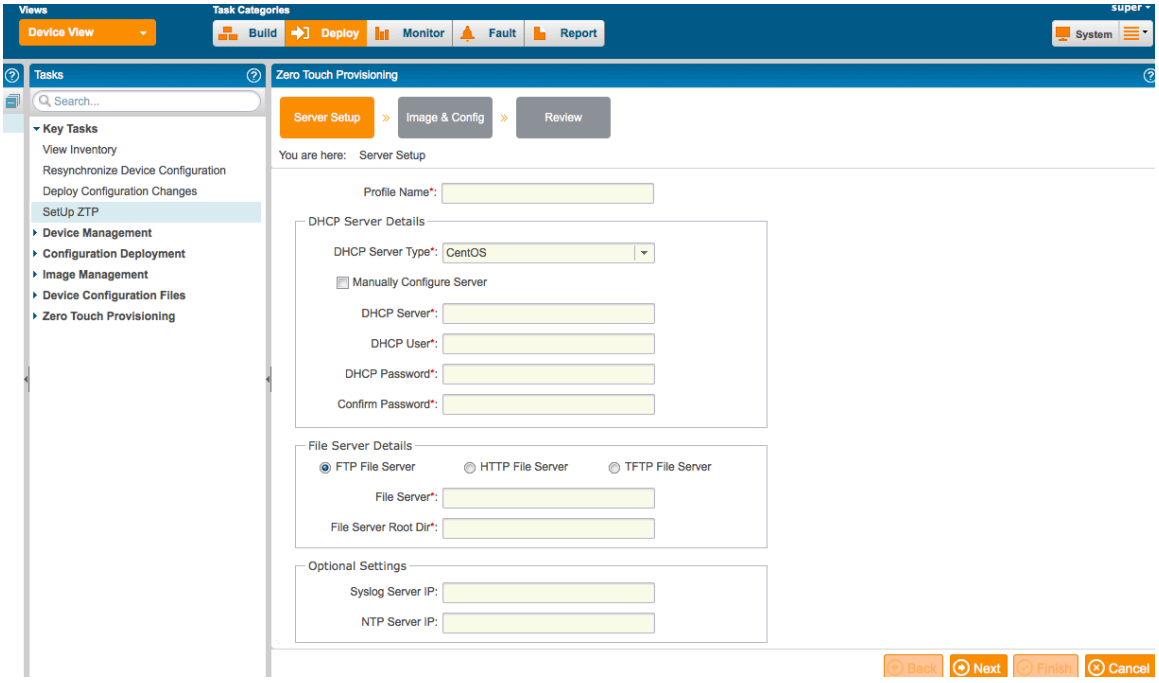
© 2016 Juniper Networks, Inc.

- Configure DHCP server for ZTP
- Prepare the basic common configuration file
- Store the necessary software images in the file server
- Store the configuration files in the file server

1. Login to Network Director and go to **Device View**



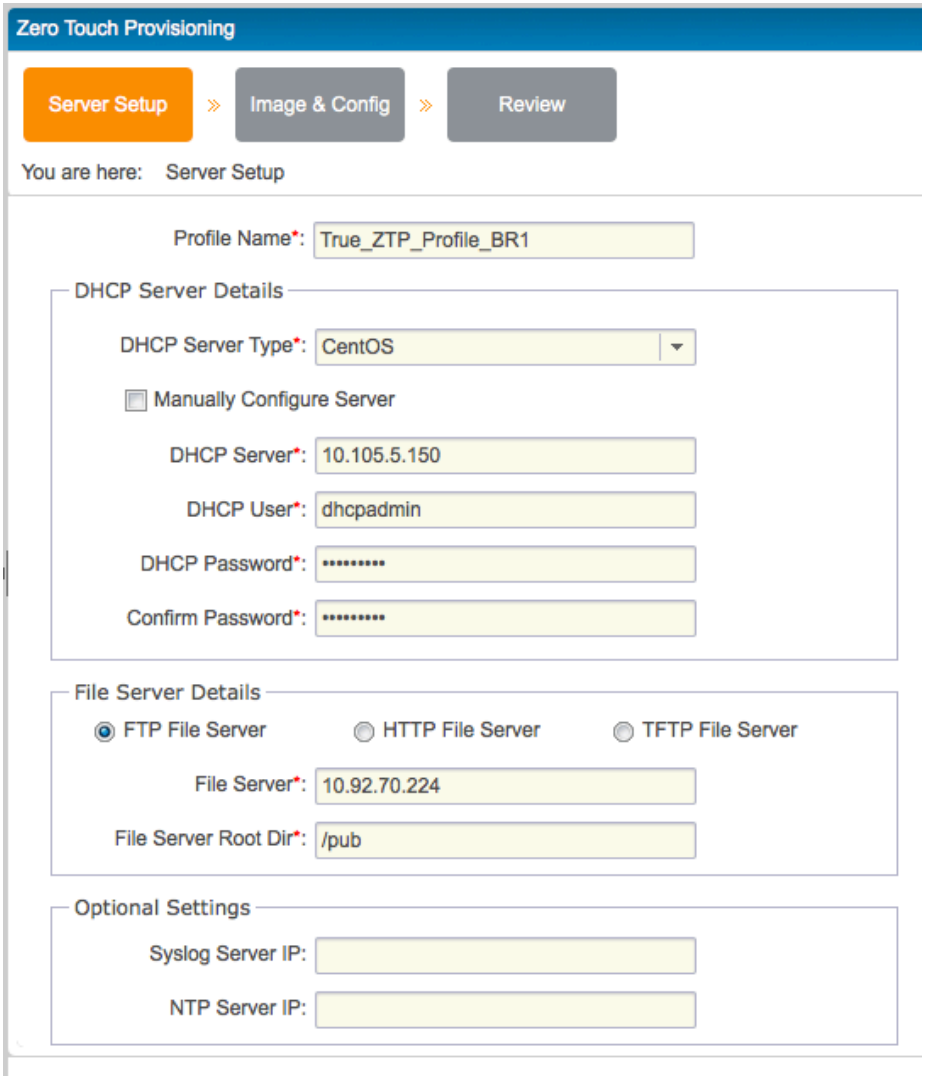
2. Select the **Deploy** task category and choose the **SetUp ZTP** task



3. Configure the parameters for ZTP setup as shown below.

© 2016 Juniper Networks, Inc.

- DHCP server details
  - Select the type of DHCP server
  - Provide DHCP server IP address
  - Provide DHCP server user and password
    - This user should have permission to edit the dhcpd.conf file
- File server details
  - Select the type of file server
    - In this example, we use FTP
  - Provide the file server IP address
    - Network Director will use “anonymous” user for FTP
  - Provide the directory to store the images and configuration files
    - Ensure that the anonymous user has read and write permissions to this directory on the FTP server
- Click **Next**



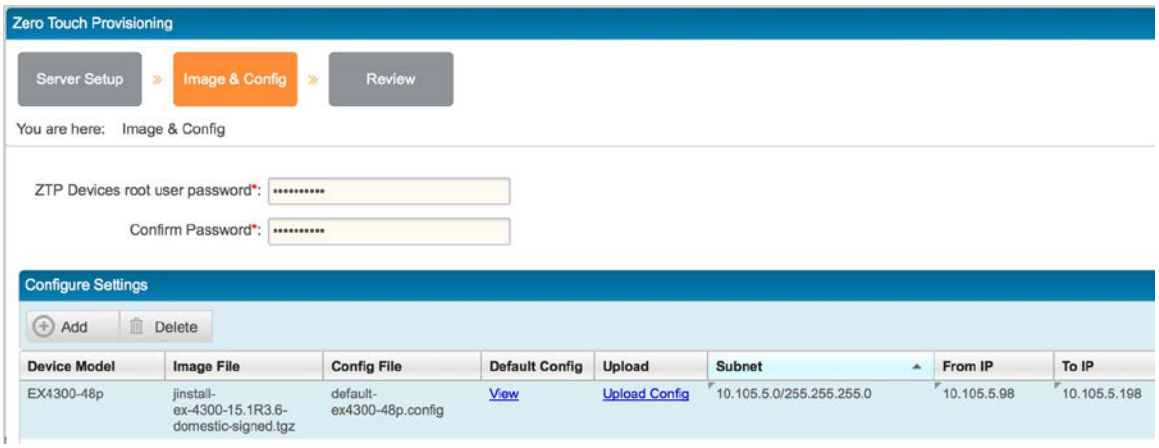
© 2016 Juniper Networks, Inc.

4. Configure the device specific parameters:

   - Configure the root password in the **ZTP Devices root user password** field
     - This will be the root password in the configuration file that the ZTP device receives during the ZTP process.
     - Please note that Network Director will use this password to discover and manage the device after the device tries to register itself with Network Director.
     - If you decide not to use the default configuration file generated by Network Director, make sure you use the same root password in the customized configuration file so the ZTP device can be managed by Network Director after the device completes ZTP and tries to register with Network Director.

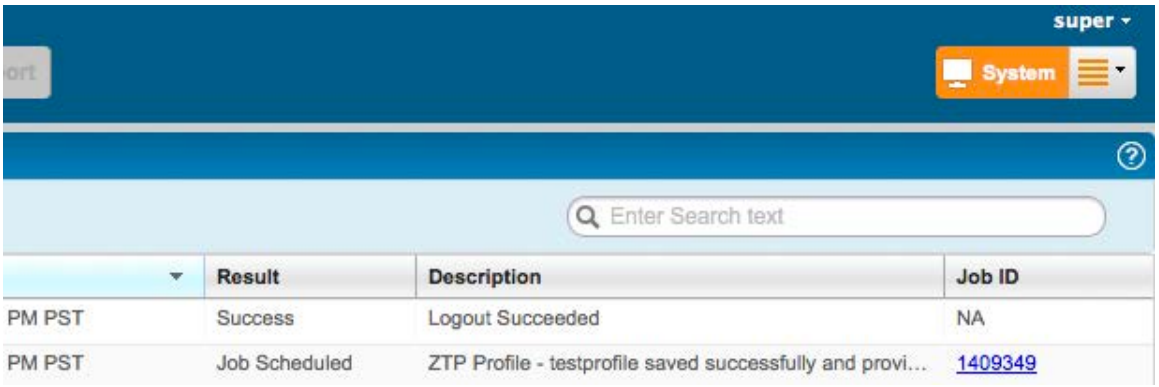
Add the type of device for which the ZTP environment should be prepared:

- Specify the device model
- Select the image you need for this device type
  - You can upload images to Network Director under **Image Management** > **Manage Image Repository**
- Upload a custom configuration file. You can see a sample configuration file at in the Appendix of this document.
  - Network Director generates a default configuration file. You can use the default configuration file or provide a custom default configuration file specific to the environment. However, in most scenarios a custom configuration file will be required to address the specific needs of the environment
- Select the subnet for the DHCP pool
  - Network Director will list the subnets that are already in the dhcpd.conf file
  - If you do not find the subnet you need, you can add a new subnet here
  - Specify the pool of IP addresses
- Click **Next**, **Review**, and **Finish**



Network Director configures the DHCP server and pushes the image file and configuration file to the FTP server. Click **System** to check the status of ZTP Profile creation job and click on the Job ID to get details on the job.

© 2016 Juniper Networks, Inc.



EX Series Switch Port Configuration

In this example, we will identify the ports that will be used for connecting Aerohive access points, and preconfigure the ports on the EX Series switch as part of the ZTP process so these ports will be ready when an AP is connected.

The following information must be predetermined:

- The ports on the switch that will be used for connecting access points. In this example, we will use interfaces ge-0/0/36 to ge-0/0/43.
- The management VLAN for the AP. In this example, we will use VLAN 10.
- Other VLANs required for the WLAN. In this example, we will use VLAN 21, 22, 23.

As part of the ZTP process, the configuration pushed down from the DHCP server will include the following configuration:

```
poe {
    interface all;
}
protocols {
    lldp {
        interface all;
    }
}
interfaces {
    interface-range AP_Ports {
        member-range ge-0/0/36 to ge-0/0/43;
        description "Aerohive Access Point";
        native-vlan-id 10;
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
                    members [ v10 v21 v22 v23 ];
                }
            }
```

© 2016 Juniper Networks, Inc.

```
        }
    }
}
vlans {
    v10 {
        description "AP Management VLAN";
        vlan-id 10;
    }
    v21 {
        description "Employee Wireless VLAN";
        vlan-id 21;
    }
    v22 {
        description "Contractor Wireless VLAN";
        vlan-id 22;
    }
    v23 {
        description "Guest Wireless VLAN";
        vlan-id 23;
    }
}
```

ZTP in Action

Unbox the switch, connect the cables, and power it up. Connect the Aerohive access points to one of the ports from ge-0/0/36 to ge-0/0/43.

If the switch is in factory default configuration, the ZTP process will automatically start. If the switch was already used, you can use the `request system zeroize` command to restore the switch to factory default state so it can enter the ZTP process.

After the switch reboots, it starts broadcasting DHCP discover packets. If a DHCP server on the network responds with a DHCP ACK packet with DHCP vendor options set with the necessary values to initiate ZTP, then ZTP proceeds.

To disable the ZTP process, manually delete the `auto-image-upgrade` statement located in the `[edit chassis]` hierarchy. If ZTP completes without errors, the auto-image-upgrade statement is automatically deleted.

The device downloads the configuration file and the image file from the file server indicated in the DHCP vendor options. The device compares the downloaded image file with the installed software version. If the downloaded image file is different from the installed software version, the downloaded software image is installed and the switch reboots.

After the software installation, the downloaded configuration file is installed and the basic ZTP process is complete. The `auto-image-upgrade` statement under the `[edit chassis]` hierarchy is deleted. This completes the basic ZTP process.

At this point, the switch has the software image required for the device and also has the common configuration file intended for that device type. The switch ports are configured and ready for AP connections.

© 2016 Juniper Networks, Inc.

Since an Aerohive AP is already connected to one of the configured ports, the AP powers up using PoE and is assigned a DHCP address on VLAN 10 (the management VLAN in this example). The AP connects to the Internet to reach HiveManager. With auto-provisioning enabled, once the AP establishes communication with HiveManager, the device will automatically receive the latest configuration and firmware.

EX Series Switch Auto-Registration with Network Director

In this example, we would also like the device to auto-register with Network Director.

- Add the following configuration to the switch's configuration file. This configuration snippet is necessary for the device to automatically register with Network Director after the ZTP process is complete. If you do not care about the device auto-registering with Network Director once the ZTP process is complete, you do not need this config snippet.

```
system {
    root-authentication {
        encrypted-password <PASSWORD>; ## SECRET-DATA
    }
}
event-options {
    policy target_add_test {
        events snmpd_trap_target_add_notice;
        then {
            raise-trap;
        }
    }
}

snmp {
    trap-group networkdirector_trap_group {
        version all;
        destination-port <ND Port>;
        categories {
            authentication;
            link;
            services;
        }
        targets {
            <ND IP Address>;
        }
    }
}
```

- Replace <*PASSWORD*> with the root password that is configured when you were setting up the ZTP profile on Network Director.
- Replace <*ND Port*> with the Network Director port. By default, this is 10162.

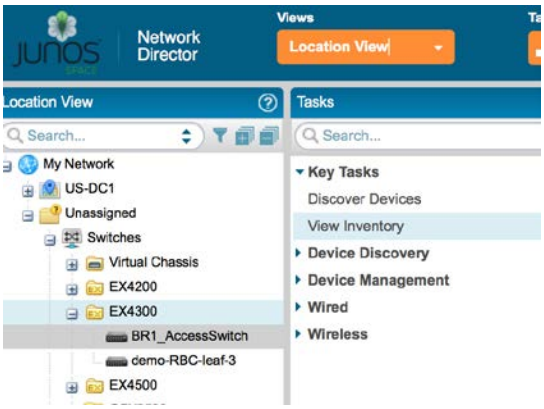
© 2016 Juniper Networks, Inc.

- Replace *<ND IP address>* with the IP address of Network Director.

NOTE: If the device should auto-register with Network Director after completing the ZTP process, the following requirements must be met:

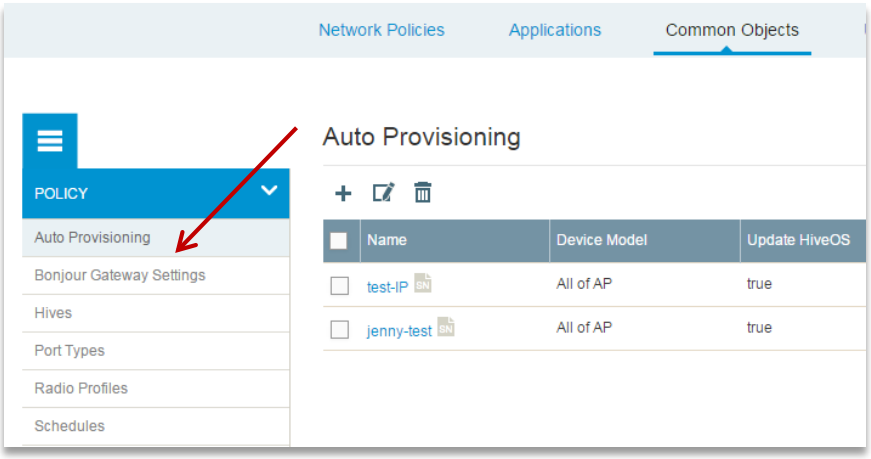
- The device should the send the trap *snmpd_trap_target_add_notice* to Network Director.
- There should be a profile on Network Director for ZTP.
- The IP address of the device must be from the pool of IP addresses defined in the ZTP profile.
- The root password of the device must be the same one that is in the ZTP profile.

After the device auto-registers with Network Director, the device can be seen in the **Unassigned** location in **Location** view. The device can then be moved by the network administrator to the appropriate location.



Aerohive Auto-Provisioning in HiveManager

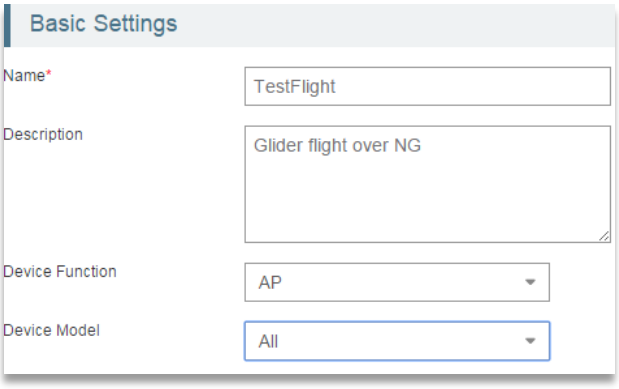
1. After the devices have been on-boarded successfully, go to the **Configure** tab > **Common Objects** and navigate to **Auto Provisioning.**



2. Click + to add the new auto-provisioning policy.

© 2016 Juniper Networks, Inc.

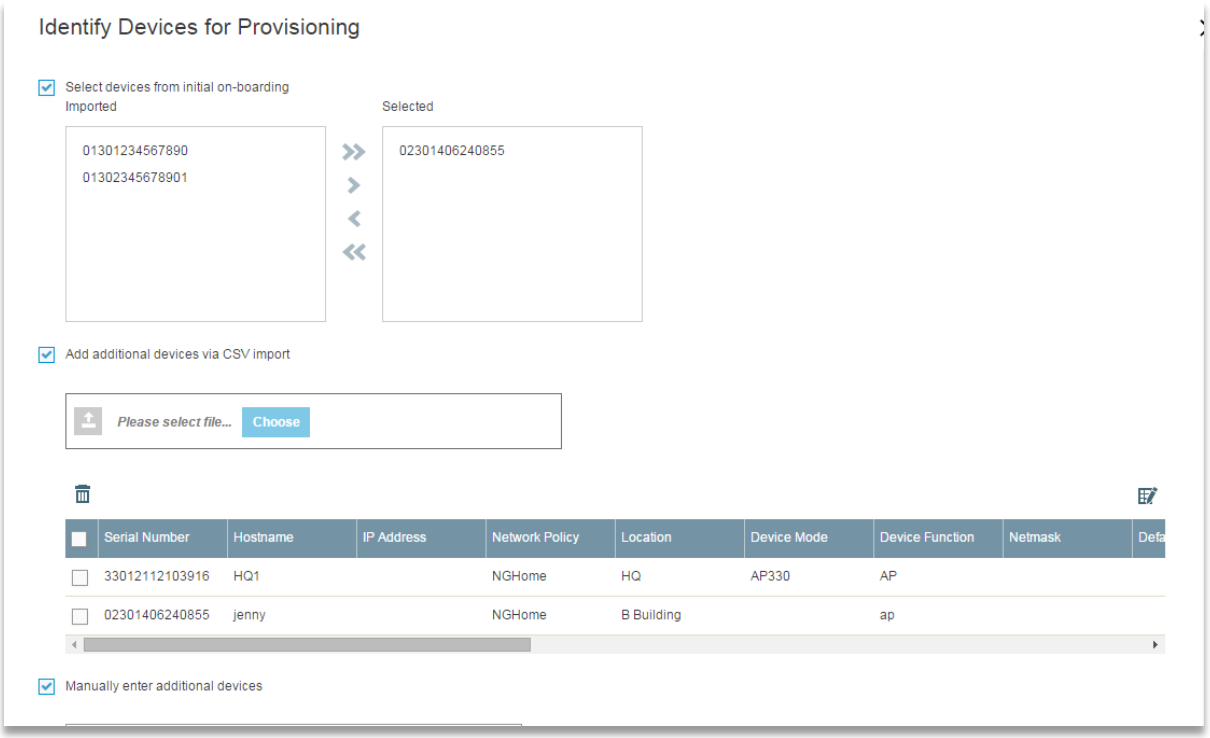
3. Name the policy, add a comment (strongly recommended), choose the device function (AP or Switch) and device model (optional, you can leave it as All).



4. To identify the devices that will be automatically provisioned, you can use the serial numbers of the previously on-boarded devices, or IP subnets.

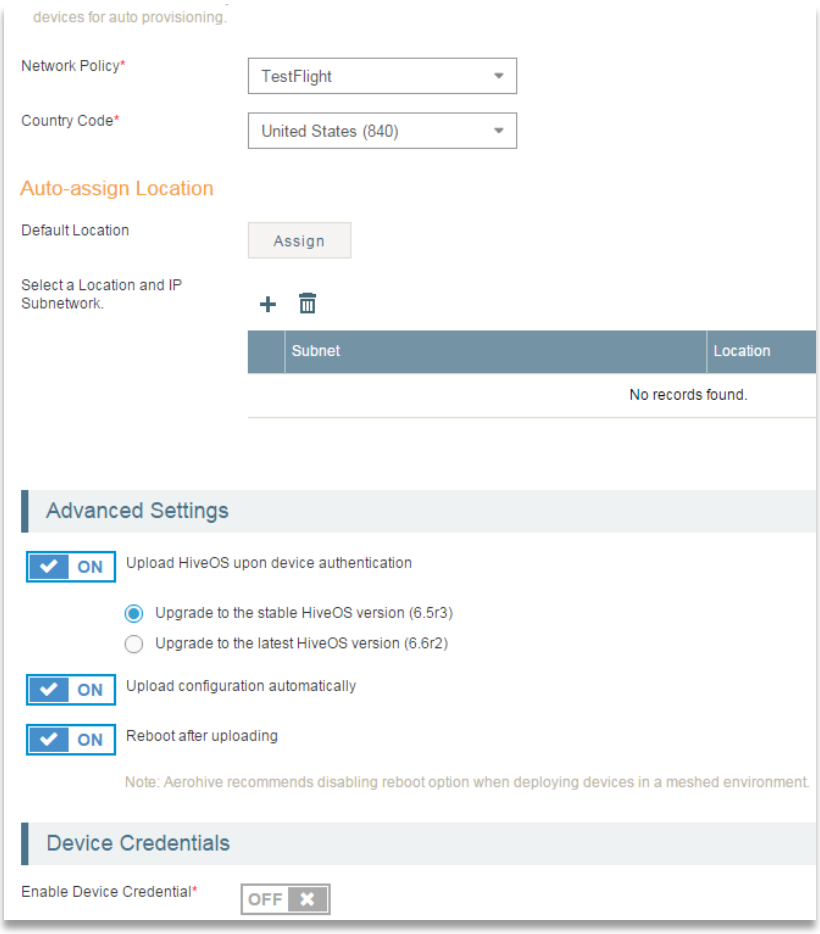
   Using serial numbers for auto-provisioning:

   - Check the Serial Numbers checkbox and click the Select Serial Numbers button.
   - You can now select serial numbers from the list of imported devices, add devices via CSV file, and/or manually add more serial numbers.



   - Click Save.
   - Choose additional settings you want to be auto-provisioned.

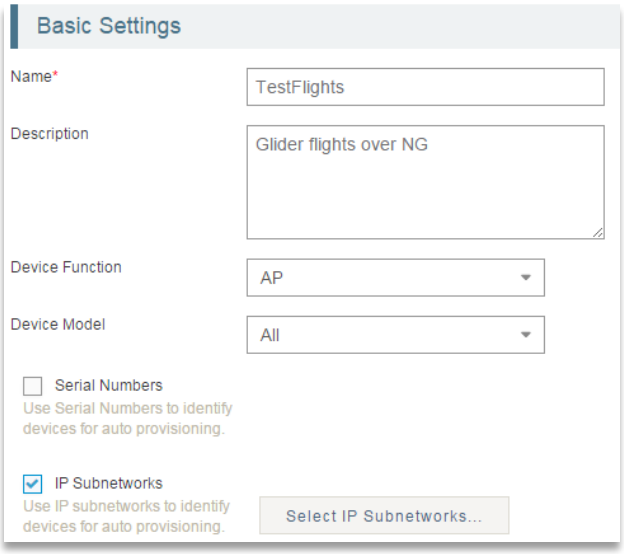
© 2016 Juniper Networks, Inc.



- Click Save.

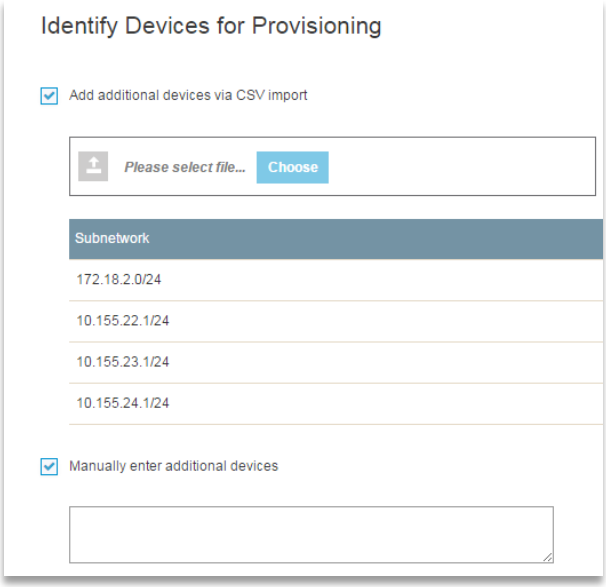
Using IP subnets for auto-provisioning:

- Check the IP Subnetworks checkbox, click Select IP Subnetworks button

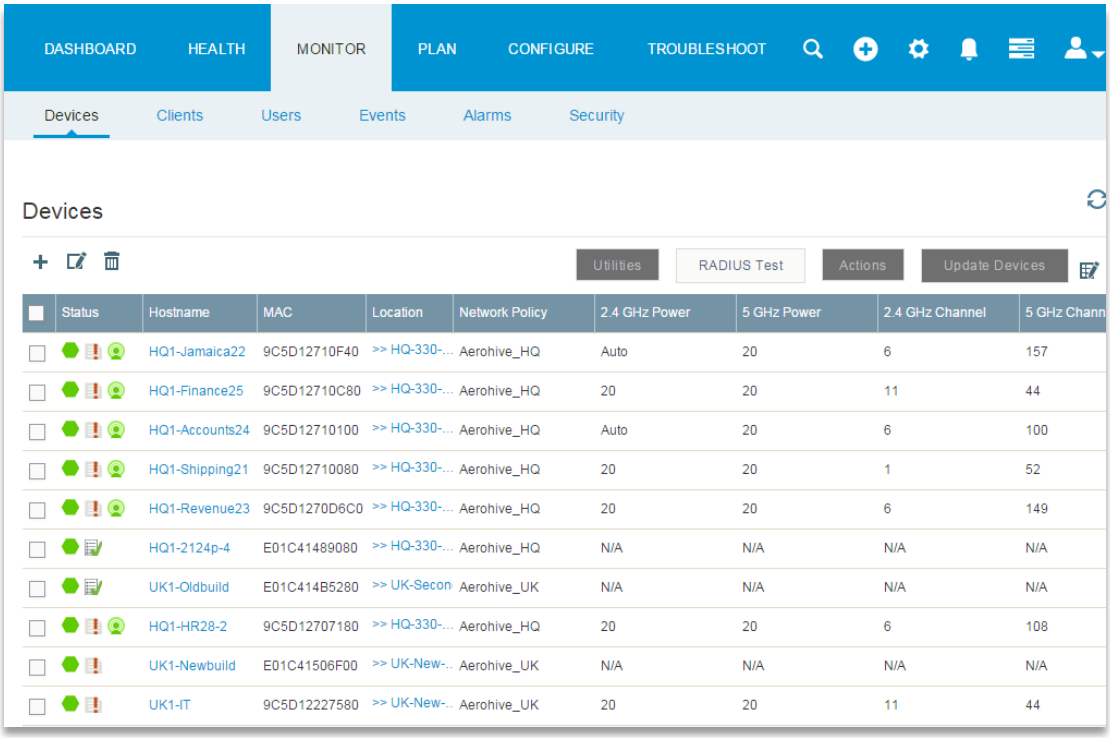


© 2016 Juniper Networks, Inc.

- Import the CSV file with the IP subnetworks or manually enter the subnet numbers.



- Click Save.
- Power on the devices.
- Go to the **Monitor** tab where you will find the devices listed. To verify that the device has been provisioned, click on the device and verify that policy and other settings are as expected. Click on the AP host name and verify that the correct network policy was applied. (You do not need to verify each and every device; we recommend “spot checks” based on location or AP model.)



© 2016 Juniper Networks, Inc.

Conclusion

The ZTP process demonstrated in this document is available on all Juniper Networks EX Series switching platforms. Aerohive access points can automatically register with Aerohive HiveManager as soon as they are plugged into EX Series switch ports configured for Aerohive APs. By combining the ZTP capabilities of Juniper's switching platforms and the auto-provisioning capabilities of Aerohive access points, enterprises have a true Zero-Touch Deployment solution for both wireless and wired network deployments. This will enable enterprises to rapidly deploy new offices or replace switches and access points without the need for manual intervention by skilled professionals.

© 2016 Juniper Networks, Inc.

Appendix – Sample Configurations

dhcpd.conf

```
ddns-update-style interim;
set vendor-string = option vendor-class-identifier;
ignore client-updates;
option space NEW_OP;
option NEW_OP.image-file-name code 0 = text;
option NEW_OP.config-file-name code 1 = text;
option NEW_OP.image-file-type code 2 = text;
option NEW_OP.transfer-mode code 3 = text;
option NEW_OP-encapsulation code 43 = encapsulate NEW_OP;
option NEW_OP.image-file-type "symlink";
option option-150 code 150 = ip-address;

class "ex4300-48" {
    match if (
        (substring (option vendor-class-identifier,0,18) = "Juniper-ex4300-48p");
    )
}

subnet 10.105.5.0 netmask 255.255.255.0 {
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option routers 10.105.5.1;
    default-lease-time 600;
    max-lease-time 7200;
    authoritative;
    pool {
        allow members of “ex4300-48”;
        range dynamic-bootp 10.105.5.98 10.105.5.198;
        option NEW_OP.transfer-mode “ftp”;
        option OPTION-150 10.92.70.224;
        option NEW_OP.config-file-name "/4300/4300-base-network.conf";
        option NEW_OP.image-file-name "/4300/ jinstall-ex-4300-15.1R3.6-domestic-
signed.tgz ";
    }
}
```

EX4300-base-network.conf

```
system {
    host-name BR1_AccessSwitch;
```

© 2016 Juniper Networks, Inc.

```
    root-authentication {
        encrypted-password <ROOT PASSWORD>; ## SECRET-DATA
    }
    services {
        rsh;
        ssh {
            max-sessions-per-connection 32;
        }
        netconf {
            ssh;
        }
        dhcp {
            traceoptions {
                file dhcp_logfile;
                level all;
                flag all;
            }
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
        file default-log-messages {
            any any;
            match "(requested 'commit' operation)|(copying configuration to
juniper.save)|(commit complete)|ifAdminStatus|(FRU power)|(FRU removal)|(FRU
insertion)|(link UP)|transitioned|Transferred|transfer-file|(license add)|(license
delete)|(package -X update)|(package -X delete) | cm_device|(Master Unchanged, Members
Changed)|(Master Changed, Members Changed)|(Master Detected, Members Changed)|(vc
add)|(vc delete)|(Master detected)|(Master changed)|(Backup detected)|(Backup
changed)|(interface vcp-) | (AIS_DATA_AVAILABLE)";
            structured-data;
        }
    }
}
```


© 2016 Juniper Networks, Inc.

```
event-options {
    policy target_add_test {
        events snmpd_trap_target_add_notice;
        then {
            raise-trap;
        }
    }
}

snmp {
    trap-group networkdirector_trap_group {
        version all;
        destination-port <ND Port>;
        categories {
            authentication;
            link;
            services;
        }
        targets {
            10.105.5.205;
        }
    }
}

interfaces {
    interface-range first24 {
        member-range ge-0/0/0 to ge-0/0/23;
        unit 0 {
            family ethernet-switching {
                vlan {
                    members v200;
                }
            }
        }
    }
    interface-range AP_Ports {
        member-range ge-0/0/36 to ge-0/0/43;
        description "Aerohive Access Point";
        native-vlan-id 10;
        unit 0 {
            family ethernet-switching {
                interface-mode trunk;
                vlan {
```

© 2016 Juniper Networks, Inc.

```
                    members [ v10 v21 v22 v23 ];
                }
            }
        }
    }
    vme {
        unit 0 {
            family inet {
                dhcp {
                    vendor-id Juniper-ex4300-48p;
                }
            }
        }
    }
}

protocols {
    igmp-snooping {
        vlan all;
    }
    rstp;
    lldp {
        interface all;
    }
    lldp-med {
        interface all;
    }
}

vlans {
    v200 {
        description “Employee Wired VLAN”;
        vlan-id 200;
    }
    v10 {
        description "AP Management VLAN";
        vlan-id 10;
    }
    v21 {
        description "Employee Wireless VLAN";
        vlan-id 21;
    }
    v22 {
```


© 2016 Juniper Networks, Inc.

```
        description "Contractor Wireless VLAN";
        vlan-id 22;
    }
    v23 {
        description "Guest Wireless VLAN";
        vlan-id 23;
    }
}

poe {
    interface all;
}
```

© 2016 Juniper Networks, Inc.