Extreme
Connect Beyond the Network

WiNG 5.X Deployment Guide

NSight Deployment

Published: March 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Contents

Overview

Wireless LAN are the lifeline of most corporate environments and is critical to business success. While they offer immense mobility and productivity benefits to the wireless users, it's often challenging for the IT managers in large organizations to monitor and manage the network.

The NSight platform provides real-time insight into your WLAN operations. You need to protect this vital business artery and the business critical data it carries, every day of the year. NSight allows you to access the wealth of information collected by Extreme Networks' WiNG operating system and visualize it through a single-pane-of-glass easy-to-use browser interface, either in real-time or over a time period of your choosing for easy trend analysis – regardless of whether you have one or more controller clusters distributed across multiple data centers.

Custom dashboards provide the right set of information for anyone in your organization. Different roles in the organization need different types of information about the WLAN. Now, you can create a custom dashboard to put that information at their fingertips, anywhere and anytime. You can give helpdesk team access to operational analytics to assist in day-to-day network troubleshooting and issue resolution. You can provide a CIO with a real-time windows into trending data for a three month period to assist in WLAN planning and budgeting. And no matter how complex the information may be, the NSight platform visualizations make it easy to read and easy to digest.

For more information about NSight features and benefits visit the following URL:

https://www.extremenetworks.com/nsight/

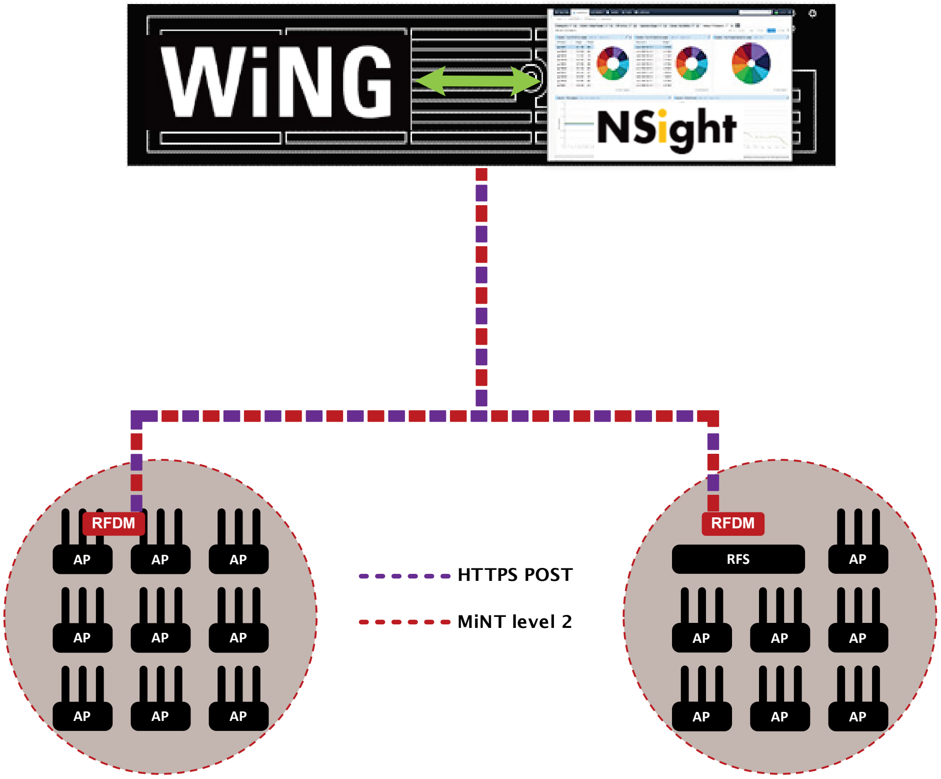
NSight Deployment Options

Zebra NSight can be deployed either on a centralized controller managing the entire WING network or as a standalone VX/NX appliance to support collecting data from multiple WiNG controller clusters to support large scale deployments up to 40,000 Access Points.

Customers interested in the NSight functionality need to ensure the centralized controller model they are investing in supports the NSight platform or deploy a standalone NSight server instance if required. Customers will need to install the NSight license with sufficient license count. The license can be ordered for a period of one to three years on per AP basis. The license cost includes the cost of software support license.

Customers Running Single WiNG Cluster (NX9XX0 / VX9000)

Customers already using a centralized controller model that supports Zebra NSight can install Zebra NSight license and configure as described in Section 2.1. Refer to scalability limits for this deployment mode in Appendix.

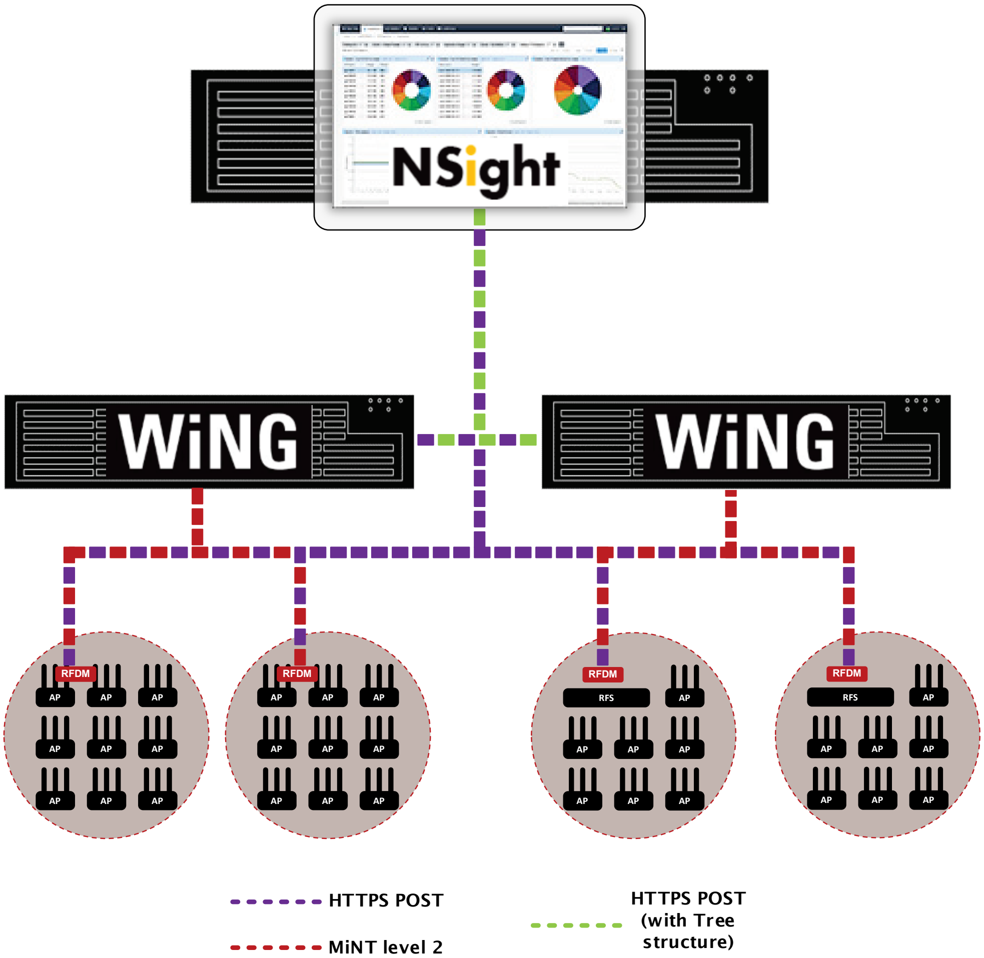


WiNG Deployment Running Multiple Clusters

Some customers may have multiple WiNG controller clusters managing large scale networks with hundreds of remote sites with more than 10,000 Access Points and controllers. In such scenarios NSight can be deployed as a standalone appliance to monitor these multiple clusters across different sites starting from WiNG release v5.8.2 as a standalone appliance or virtualized instance.

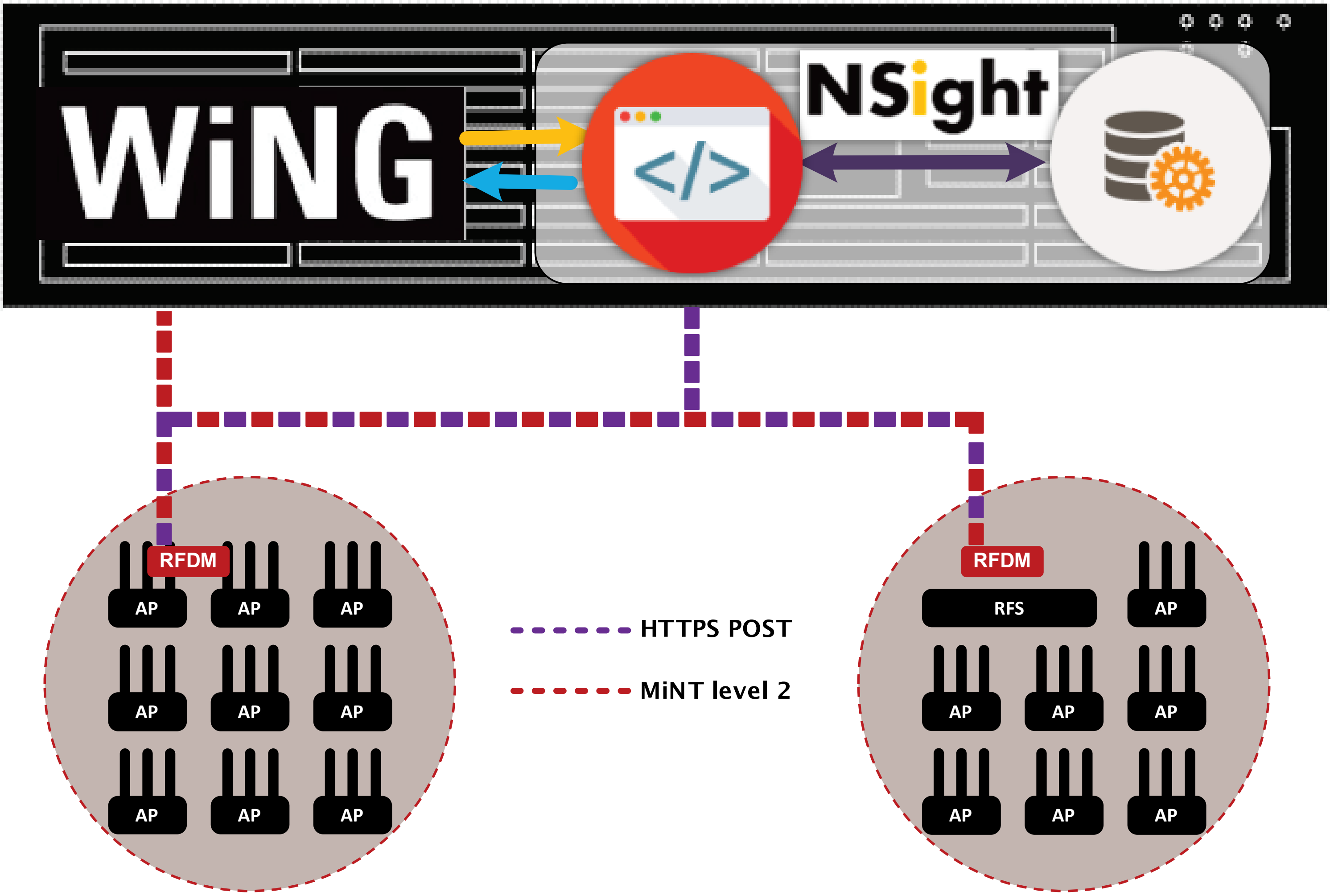
Additionally this deployment model will also suit customers running legacy RFSX000 controllers managing remote sites.

As a rule of thumb it is recommended to deploy NSight in standalone mode when the number of APs deployed is 3,000 or more.



Nsight Architecture – Integrated WiNG & Nsight

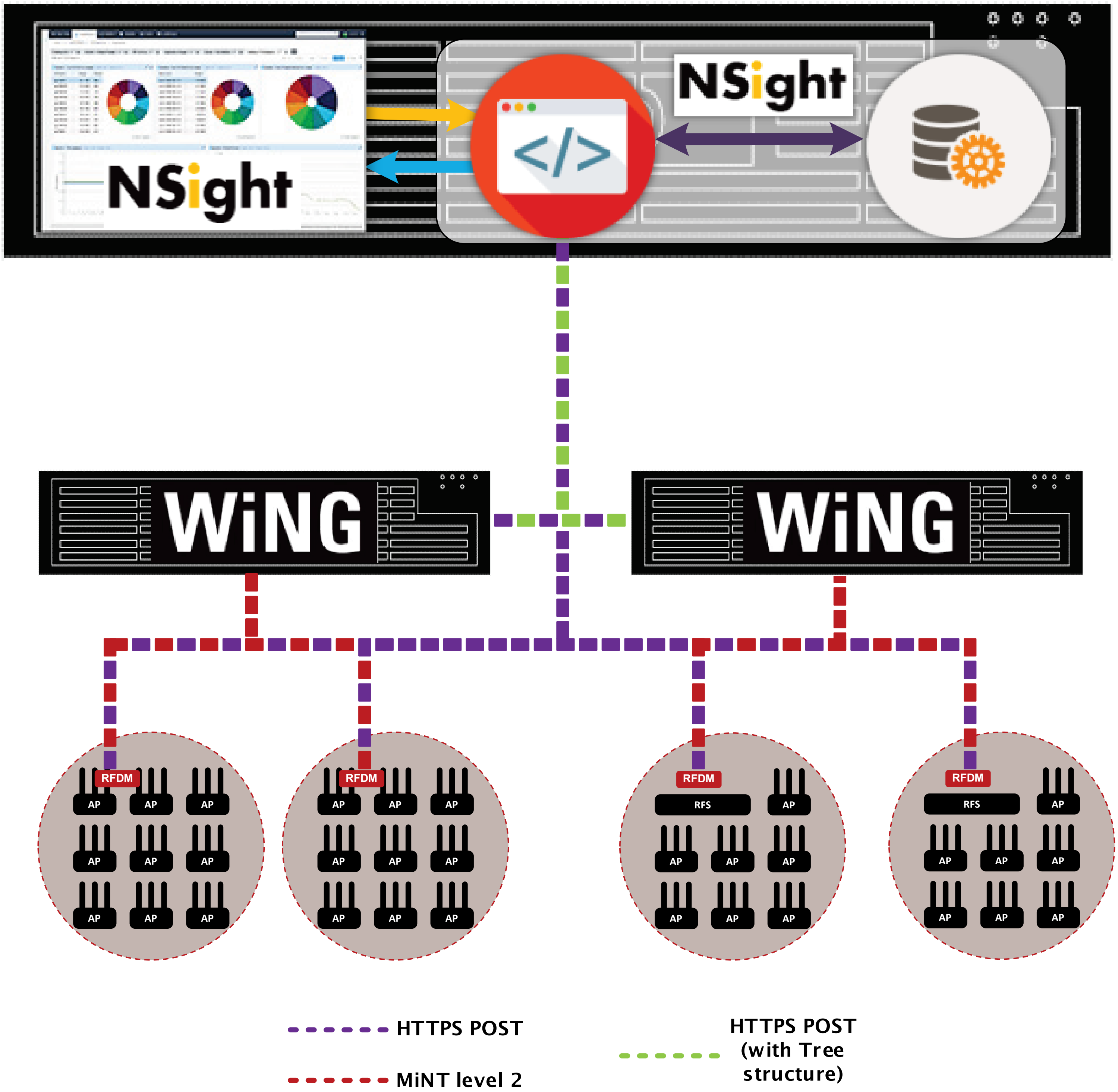
The NSight component runs on the NOC controller along with existing WiNG Management modules. The NSight module interacts with the WiNG Controller Module and the Access Points to exchange statistics and configuration information.



As before, the Access Points communicate with the WiNG Module for their management needs via MiNT protocol. In addition, they also post additional statistics with the NSight Server via Websocket.

NSight Architecture – NSight Standalone Server

The NSight server runs on a standalone VX or NX9XXX platform without any WiNG management functions enabled. The NSight module only receives statistics and configuration information from remote sites. Additionally, each WiNG NOC controller will send information about the configuration tree structure. Standalone NSight server does not interact with the WiNG Module on the same controller and does not report any statistics for itself to NSight.



There are a few differences when it comes to the NSight running in standalone mode:

- In standalone mode the controller does NOT manage any other devices or their configuration.
- NSight server only collects statistics, events and relevant configuration updates from multiple sites and provides unified access to the collected information via NSight UI:

NSight server aggregates configuration information received from remote sites.

NSight server aggregates statistics received from remote sites (same as onboard NSight).

Standalone NSight server does not report its own configuration.

Standalone NSight server does not report its own statistics.

- NSight client running on the main NOC controller also reports configuration tree information to standalone NSight server. Controller adoption must be disabled on each NOC controller, otherwise it will not report tree information back to NSight.
- Standalone NSight database only supports replica set deployments if redundancy is required. WiNG clustering as a mean to achieve database redundancy is not supported.

NSight Core Components

NSight Server

The NSight Server is a web application. It interacts with the WiNG Management module and the RF domain managers from each site and performs the following functions:

- Automatically receives configuration updates from the WiNG Management Module
- Receives statistics updates from all the RF Domain Managers periodically
- Receives Adoption information from the NOC and site controllers
- Manages and serves API requests from the front end

NSight Client

The NSight Client functionality resides on the RF Domain Managers for each site. The RF-Domain manager could be a dynamically elected access point or a local site controller. The NSight Client collects statistics from all the Access Points in the RF Domain, aggregates them and sends to the NSight Server every 60 seconds by default (see configuration chapter for additional details on nsight update intervals).

The RF Domain Manager sends the following statistics to the NSight Server:

- AP statistics: per radio and per WLAN stats. Utilization, channel, RF health, etc
- Client statistics: Client utilization, device details, etc
- Wired statistics: Ethernet port utilization, error rate, etc.
- Event History: The Event history from each device.
- Alarm Information: Alarm events from each device.
- Adoption information: Sent if the RF Domain Manager is a site controller.

NSight Database

The NSight server stores the information and statistics into the Database (MongoDB). The database stores information on all the wireless clients, APs and controllers seen on the network.

- The devices are uniquely identified by their MAC address
- All information about the devices are stored – e.g. MAC, IP, hostname, firmware, location
- Smart-RF neighbor information from each AP radio

- Rogue APs detected on the network
- Client statistics: client counts, Utilization, applications, etc.
- AP statistics: per port, per Radio and Per WLAN statistics
- Event history from each device.
- Alarms from each device

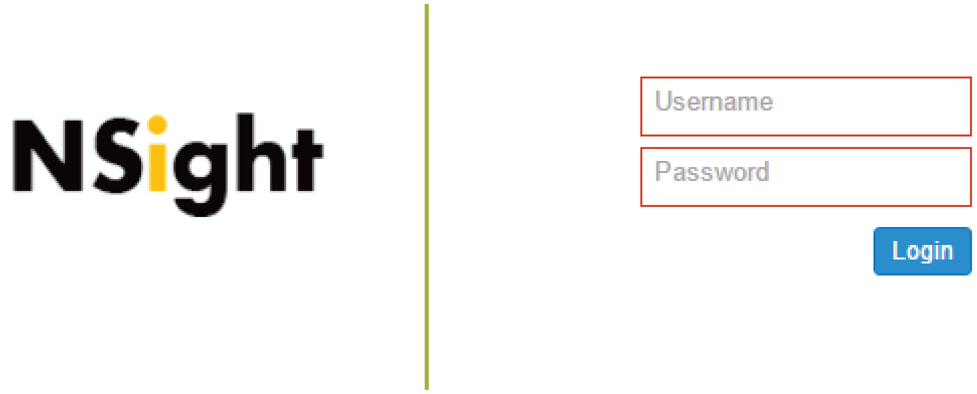
NSight database supports high availability and redundancy via replica sets. Refer to Configuration chapter for deployment details.

NSight User Interface

The NSight supports a user friendly interface that is exceptionally responsive.

The NSight User Interface can be launched directly from the browser with the URL https://<ip-address | fqdn>/nsight-ui/

This login screen can be used to provide multi-tenant view access to users based on site or location tree configuration. See Configuration section for more details.



Single Sign-on: Alternatively, the *NSight UI* can be launched from the WiNG5 Flex UI using single sign-on. The benefit of single sign-on is that the user does not need to log in again on the NSight UI.

Licensing

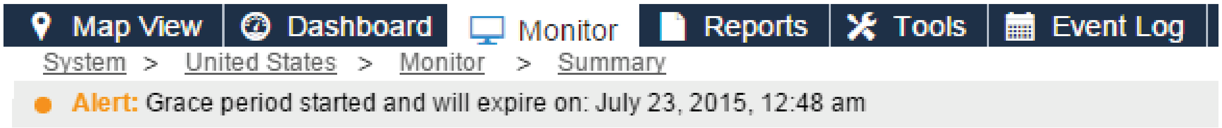
The NSight feature is a licensable feature which follows a subscription model.

The license key comprises of two key parameters: device count & expiry date:

Device count: The count should be equal or more than the number of managed devices in the network, and is a sum of the total number of Access Points and Controllers.

Expiry Date: The licenses are valid till the expiry date specified on the licenses. The Licenses are available for a period of 1 to 3 years.

If the license count is insufficient or the licenses have expired, a warning message is displayed on the NSight UI for a period of 60 days, as shown below. After 60 days, the NSight User Interface is shut down. After the UI is shut down, NSight server will continue to collect statistics and write information to the database. Once required licenses will be added NSight UI will resume normal operation.



Alert: Grace period started and will expire on: July 23, 2015, 12:48 am

NSight integrated with WiNG controller:

A license needs to be installed on the NOC controller running NSight and is shared amongst the cluster members.

NSight as a standalone server:

A license needs to be installed on the primary replica set member running NSight and is shared amongst mongodb replica set members. License must be installed only on the primary member.

Note
VX9000 acting as a standalone NSight server does not require VX platform license. Only NSight licenses should be installed.

Database Redundancy – Database Replica Set

WiNG 5.8.2 release added support for 3 node replica set option for High Availability deployment of standalone NSight or Captive Portal Registration database. This is a recommended HA deployment model starting from WiNG 5.8.2 onwards for any NSight deployment model.

Note
Previously in versions 5.8.0 and 5.8.1 WiNG clustering was used to achieve database redundancy. This model is not supported starting from WiNG 5.8.2.0

- Database redundancy is decoupled from WiNG clustering.
- Database replica set must always have an odd number of nodes:

A standalone instance (standalone NX/VX running mongodb)

A replica set with 2 (or more) full-nodes and 1 arbiter

A replica set with 3 (or more) full-nodes

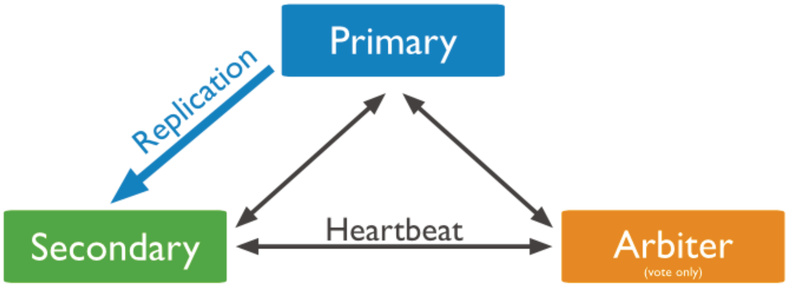
Terminology

Replica set - a group of database processes that maintain the same data set. Replica sets provide redundancy and high availability, and are the basis for all production deployments.

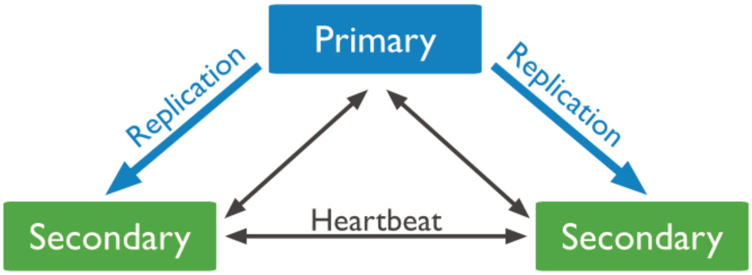
Full-node – a database replica set member with full copy of the data.

Arbiter – a lightweight database server process which stores no data, it participates in replica set heart beats and primary database elections. The sole purpose of arbiter is to break a tie when database election process is happening and ensure database contents of the primary are the “freshest” ones.

Replica sets with 2 or more full-nodes and an arbiter:



Replica sets with 3 or more full-nodes:



NSight Configuration

There are two parts to the NSight Configuration. First is NSight server which is defined by the nsight policy configuration applied either to the NOC controller or a standalone VX/NX platform depending on the deployment. Another part is NSight client which is defined by a separate nsight policy configuration assigned to each RF Domain.

NSight Server – Integrated with WiNG controller:

To enable NSight server running along with WiNG Controller on NX9XX0 or VX9000 controller an **NSight Server Policy** must be created and assigned to the RF-Domain of the NOC controller or directly assigned to the controller as a Device Override. Also default database policy must be assigned to the VX or NX controller in order to start the database process.

> **Note**
>
> This configuration is available in CLI mode only. In case NSight server has management access restriction enabled it must permit source IP subnet of the Access Points as well to allow HTTPS socket to establish.

NSight server policy configuration example:

```
!
nsight-policy ONBOARD-SERVER
 nsight-server
!
database-policy default
!
```

Policy assignment to the NOC controller:

```
!
nx9600 B4-C7-99-11-32-43
 use profile centralized-nx9600
 use rf-domain NOC
 hostname NX96-CTRL-1
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 license NSIGHT 7368eb295c87e469389ce8c43179a09dd6ec4f96339feda1e243e03ac05bb97c70a814fb548101ad
 trustpoint https noc
 use database-policy default
 use nsight-policy ONBOARD-SERVER
 interface vlan1
  ip address dhcp
 use event-system-policy DB
 ntp server time.nist.gov
!
```

NSight Server – Standalone Server:

To enable NSight server running on a standalone VX or NX appliance an NSight Server Policy must be created and assigned to the VX/NX controller acting as a standalone NSight server. Also default database policy must be assigned to the VX or NX controller in order to start the database process. Special “standalone” mode must be specified to designate an appliance to run NSight services only.

> **Note**
>
> Configuration is available in CLI mode only. In case NSight server has management access restriction enabled it must permit source IP subnet of the Access Points as well to allow HTTPS socket to establish.

NSight server policy configuration example:

```
!
nsight-policy STANDALONE-SERVER
 nsight-server standalone
!
database-policy default
!
```

Policy assignment to the standalone server:

```
!
vx9000 06-71-B1-5D-77-51
 use profile default-vx9000
 use rf-domain default
 hostname NSIGHT-PRIMARY
 license ADSEC DEFAULT-ADV-SEC-LICENSE
 license NSIGHT 7368eb295c87e469389ce8c43179a09dd6ec4f96339feda1e243e03ac05bb97c70a814fb548101ad
 trustpoint https noc
 use database-policy default
 use nsight-policy STANDALONE-SERVER
 interface vlan1
  ip address dhcp
 use event-system-policy DB
 ntp server time.nist.gov
 logging buffered debugging
!
```

NSight Client Configuration

To enable NSight client functionality and allow the RF Domain Manager to report statistics to NSight server an NSight Client Policy is created and assigned to the RF-Domain of each site that shall report statistics to NSight. The NSight policy is configured with the IP address of one or two NSight servers on which the NSight Server is running. The NSight client (RF Domain Manager) will try the first IP address that is configured in the NSight policy. If it fails to reach the first IP address, then it tries the second IP address.

> **Note**
>
> NOC Controller that is managing Access Points must have “controller adoption” disabled in order to send configuration tree information to the NSight server. It is enabled by default on RFSX000 and smaller sized NX Series Controllers. Same applies for NOC-less deployments with multiple standalone sites managed by RFS/NX controllers.

NSight server policy configuration example:

```
!
nsight-policy REMOTE-SITES
 server host <IP address | FQDN of the nsight server> <http | https>
 server host <IP address | FQDN of the nsight server> <http | https>
!
```

Policy assignment to the RF Domain:

```
!
rf-domain BRANCH-1
 geo-coordinates 49.1974 16.6002
 contact cgj864@extremenetworks.com
 timezone Europe/Prague
 country-code cz
 use smart-rf-policy SMRT
 use wips-policy WIPS
 use nsight-policy REMOTE-SITES
 sensor-server 1 ip adsp.extremenoc.com
 layout area APS floor Floor4 map-location floorplan.jpg units meters
 layout area APS
 tree-node country "Czech Republic" city Brno campus LAB
 control-vlan 1
!
```

NSight High Availability Deployment

When redundancy and high availability is required database replica sets can be deployed to ensure CAP can be achieved (consistency, availability and partition tolerance of data).

To provide data redundancy and application high-availability, a replica set configuration is required. A replica set requires 3 members, ideally 1 in each in a data center, assuming more than 2 data centers exist. If no third data center is available, it is preferable that the third member is located in some external location to prevent a single point of failure by having 2 members in the same data center. If a third location is not possible, it is preferred that the third member be placed in the primary data center.

TCP port 27017 is required to be open for inter-database communication between all replica set members.

This guide will cover both standalone database and replica set deployments.

Standalone Database - No Redundancy

Enabling NSight server on a VX/NX appliance will automatically start the database server in a “standalone” mode. No data redundancy is provided in standalone mode. NSight and Captive-Portal can be used in standalone mode without any further database specific configuration.

Replica Set Deployment with an Arbiter

In this scenario replica sets consist of at least a primary, one or more secondary servers and an arbiter. An arbiter is a lightweight database server process which stores no data, it participates in replica set heart beats and primary elections. Arbiters are good candidates for location outside of a data center as their data requirements are light, and the external location provides prevents the single point of failure scenario previously mentioned.

The primary and secondary devices **must** be of the same device type: NX9600-NX9600, NX9500-NX9500, VX9000-VX9000, NX7500-NX7500 (Captive-portal database only).

Arbiters may be any device type that supports the arbiter role: NX9600, NX9500, VX9000, NX7500, NX5500.

Configuring Replica Set with an Arbiter:

1. Identify the tree devices which will be used to form the replica set.
2. Identify the primary and secondary devices. If using a single secondary, the third device will be an arbiter.
3. On each device create a database policy. It is recommended to statically set priorities for primary and secondary. Default priority is 1, higher number wins:

```
PRIMARY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config)#database-policy replica-set
PRIMARY(config-database-policy-replica-set)#replica-set member primary.extremenoc.com priority 200
PRIMARY(config-database-policy-replica-set)#replica-set member secondary.extremenoc.com
PRIMARY(config-database-policy-replica-set)#replica-set member arbiter.extremenoc.com arbiter
PRIMARY(config-database-policy-replica-set)#end
PRIMARY#commit write
```

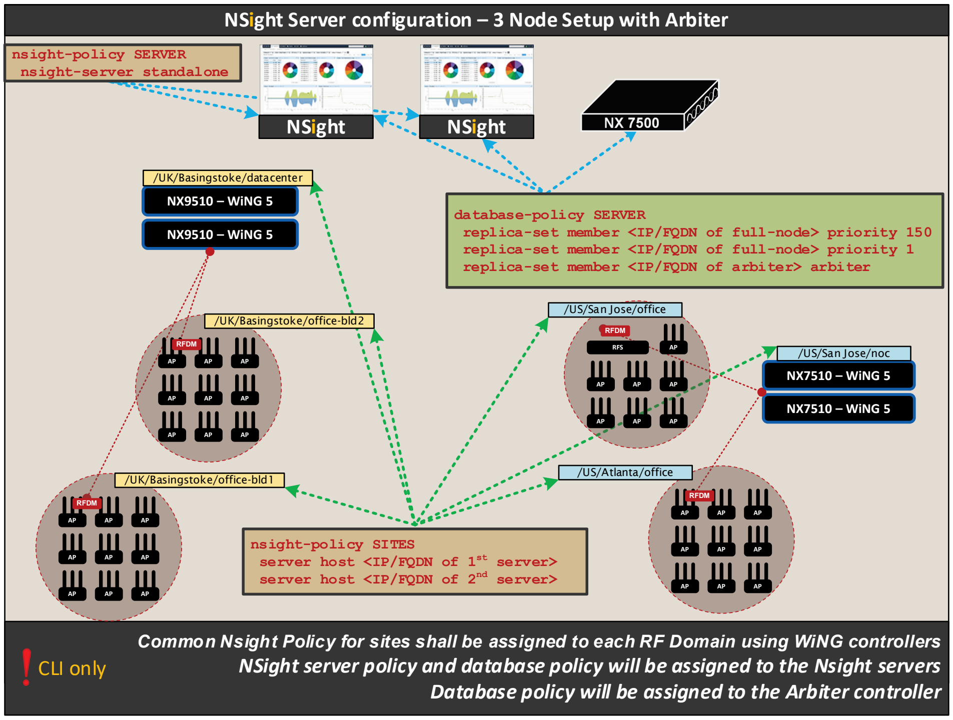
4. Apply the database policy to each device. The order does not matter.

```
PRIMARY#self
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config-device-08-00-27-11-C2-DD)#use database-policy replica-set
PRIMARY(config-device-08-00-27-11-C2-DD)#end
PRIMARY#commit write
```

5. Check database status on the device

```
PRIMARY#show database status
--------------------------------------------------------------------------------
          MEMBER                      STATE                      ONLINE TIME
--------------------------------------------------------------------------------
  172.31.0.49*            PRIMARY              8 hours 9 min 12 sec
  172.31.2.248            SECONDARY            8 hours 9 min 4 sec
  172.31.5.121            ARBITER              8 hours 9 min 8 sec
--------------------------------------------------------------------------------
[*] indicates this device.
```

When the show database status output looks like that in step 5, a replica set has been configured, applied and formed. The asterisk [*] in the output indicates the device on which “show database status” was executed.



NSight Server configuration – 3 Node Setup with Arbiter

```
nsight-policy SERVER
 nsight-server standalone
```

```
database-policy SERVER
 replica-set member <IP/FQDN of full-node> priority 150
 replica-set member <IP/FQDN of full-node> priority 1
 replica-set member <IP/FQDN of arbiter> arbiter
```

```
nsight-policy SITES
 server host <IP/FQDN of 1st server>
 server host <IP/FQDN of 2nd server>
```

Common Nsight Policy for sites shall be assigned to each RF Domain using WiNG controllers
NSight server policy and database policy will be assigned to the Nsight servers
Database policy will be assigned to the Arbiter controller

Replica Set Deployment with Full Nodes

Configuring replica set with Full Nodes Only:

1. Identify the tree devices which will be used to form the replica set.
2. Identify the primary device, all other devices will be secondary. Total number of devices must be odd.
3. On each device create a database policy. It is recommended to statically set priorities for primary and secondary. Default priority is 1, higher number wins:

```
PRIMARY#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config)#database-policy replica-set
PRIMARY(config-database-policy-replica-set)#replica-set member primary.extremenoc.com priority 200
PRIMARY(config-database-policy-replica-set)#replica-set member secondary.extremenoc.com priority 15
PRIMARY(config-database-policy-replica-set)#replica-set member tertiary.extremenoc.com priority 5
PRIMARY(config-database-policy-replica-set)#end
PRIMARY#commit write
```

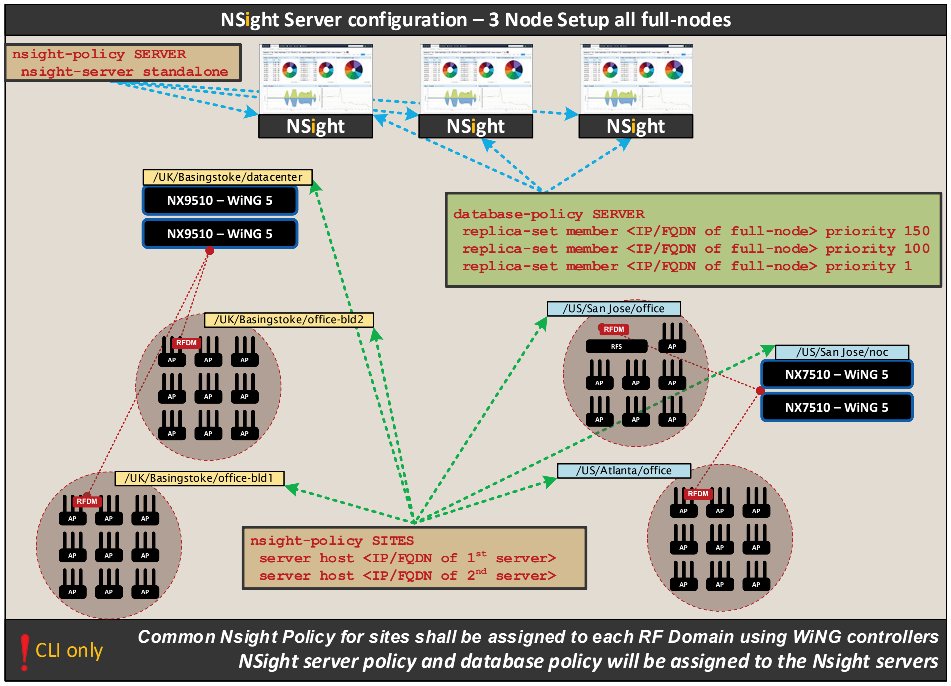
4. Apply the database policy to each device. The order does not matter.

```
PRIMARY#self
Enter configuration commands, one per line.  End with CNTL/Z.
PRIMARY(config-device-08-00-27-11-C2-DD)#use database-policy replica-set
PRIMARY(config-device-08-00-27-11-C2-DD)#end
PRIMARY#commit write
```

5. Check database status on the device

```
PRIMARY#show database status
--------------------------------------------------------------------------------
          MEMBER                 STATE                        ONLINE TIME
--------------------------------------------------------------------------------
  172.31.0.49*             PRIMARY              8 hours 9 min 12 sec
  172.31.2.248             SECONDARY            8 hours 9 min 4 sec
  172.31.5.121             SECONDARY            8 hours 9 min 8 sec
--------------------------------------------------------------------------------
[*] indicates this device.
```

NSight Server configuration – 3 Node Setup all full-nodes



```
nsight-policy SERVER
 nsight-server standalone
```

```
database-policy SERVER
 replica-set member <IP/FQDN of full-node> priority 150
 replica-set member <IP/FQDN of full-node> priority 100
 replica-set member <IP/FQDN of full-node> priority 1
```

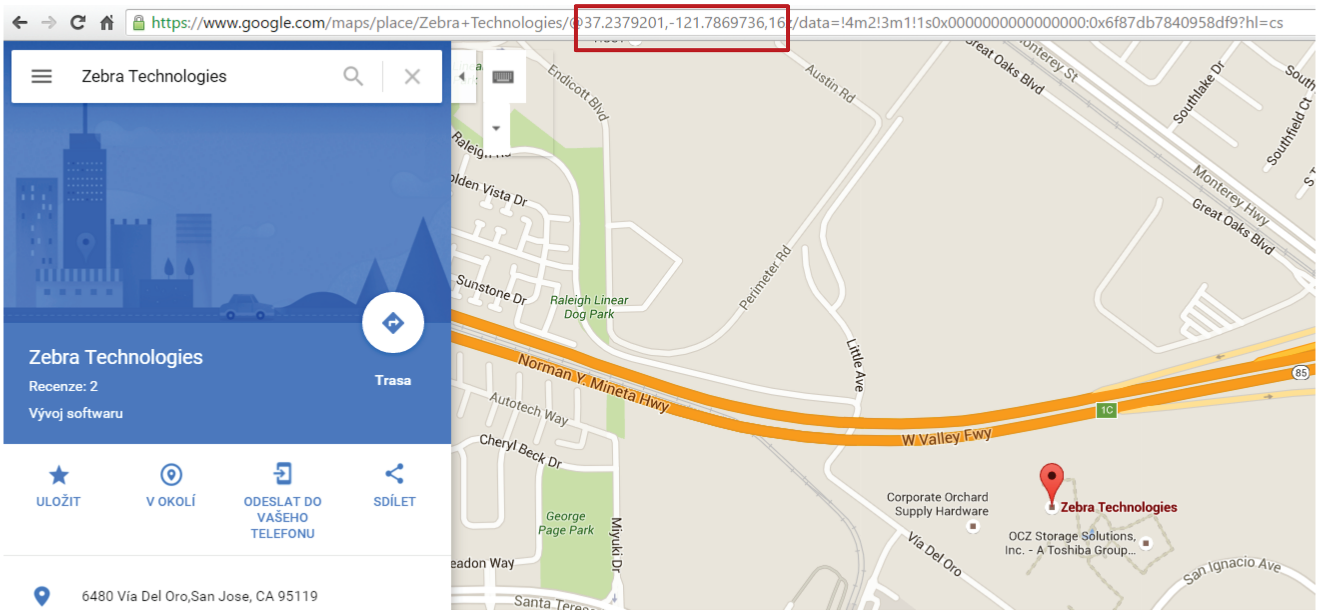
```
nsight-policy SITES
 server host <IP/FQDN of 1st server>
 server host <IP/FQDN of 2nd server>
```

Common Nsight Policy for sites shall be assigned to each RF Domain using WiNG controllers
NSight server policy and database policy will be assigned to the Nsight servers

Placing RF Domains on a Map in NSight

One of the configuration required on the WiNG infrastructure side for NSight global Map View is setting up the geo coordinates for each RF Domain. Once NSight will obtain correct geo coordinated mapped to a specific RF Domain it will place this site on a global Map View.

1. Find exact Geo coordinates of the RF Domain using any service, for example Google Maps. Just search for an address, Geo Coordinates will be shown in the URL as in example below:

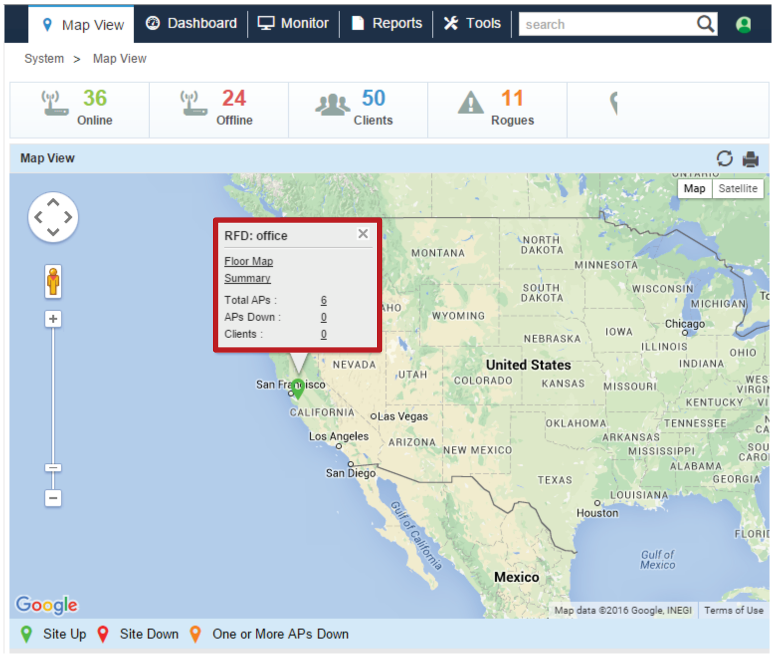


https://www.google.com/maps/place/Zebra+Technologies/@37.2379201,-121.7869736,16z/data=!4m2!3m1!1s0x0000000000000000:0x6f87db7840958df9?hl=cs

2. Put Geo coordinates into the Location field under RF Domain configuration. This configuration item is available in CLI only.

```
!
rf-domain office
 geo-coordinates 37.2379 -121.7870
 country-code us
 use smart-rf-policy SMRT
 use wips-policy WPS
 use nsight-policy REMOTE-STANDALONE
 control-vlan 1
!
```

4. Once WiNG Conroller will report new Location value to the NSight server, RF domain will correctly display on the Map View:



RFD: office

Floor Map

Summary

Total APs : 6

APs Down : 0

Clients : 0

Floor Maps in NSight

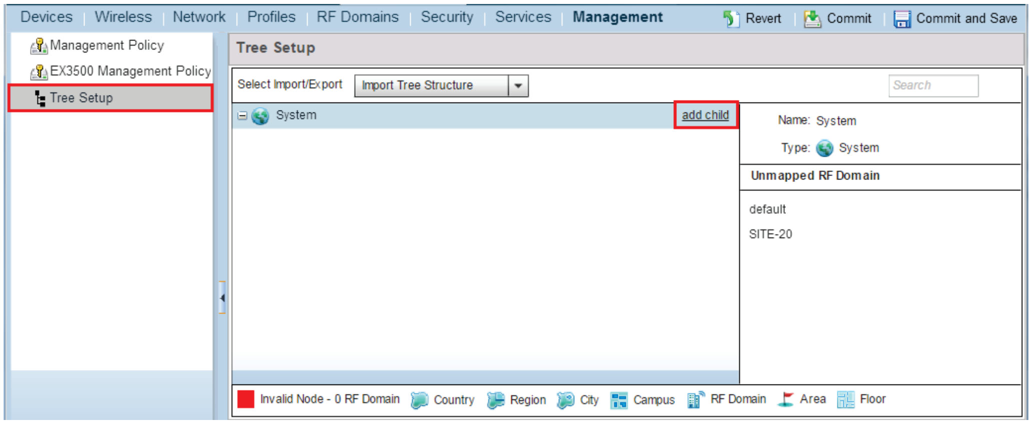
The floormaps should be defined in WiNG5 using Floors and Areas in order to be displayed in NSight. Access Points can be places on a floormap using NSight UI. Additionally, it is recommended to configure Tree Hierarchy in WiNG for better visibility of each RF Domain based on geographical location.

The WING deployments can be organized in a tree hierarchy to reflect the real life network. It also makes it convenient to browse the wireless network when organized in this manned compared to looking for individual RF-domains. When using NSight, if a user has selected a higher level object in the tree hierarchy, the user can see consolidated information from all the RF Domains under that location hierarchy.

The tree can be organized into multiple network levels – Country, Region, City or Campus. Network Administrator can create a tree hierarchy to be consistent with the wireless deployment.

Refer to the configuration steps below as an example:

1. Go to **Configuration** > **Management** > **Tree Setup**. Click **Add Child**.



Tree Setup

Select Import/Export: Import Tree Structure

System

Name: System

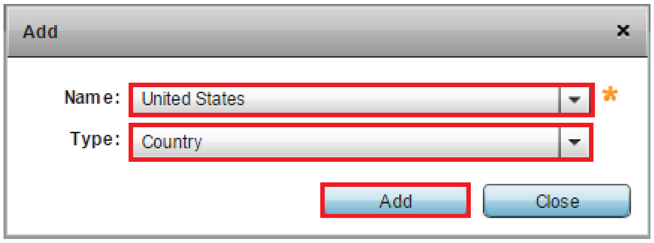
Type: System

Unmapped RF Domain

default

SITE-20

2. Select the **Country**. Click **Add**.

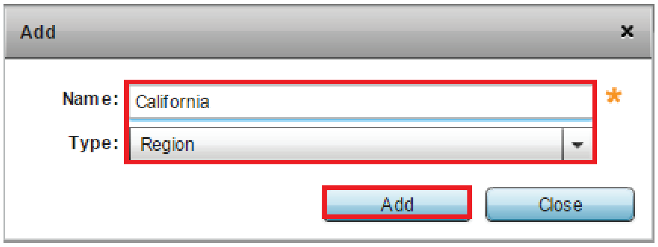


Add

Name: United States *

Type: Country

3. Click **Add Child** and configure the region **California**. Click **Add**.

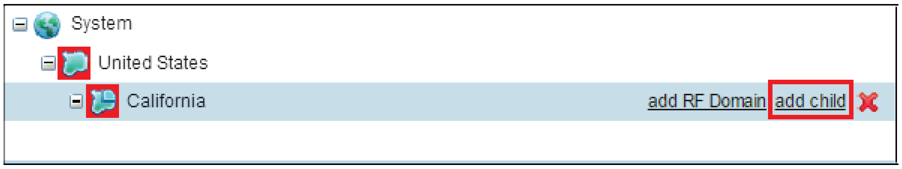


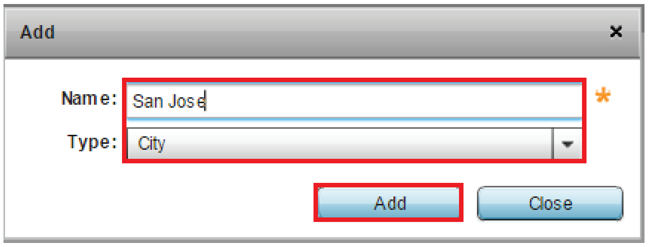
Add

Name: California *

Type: Region

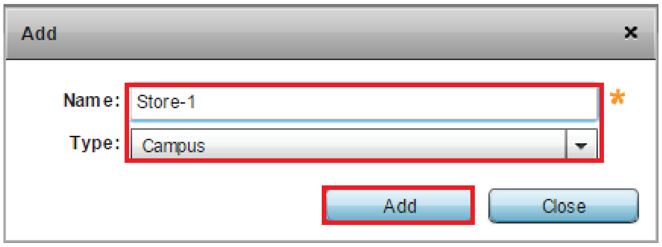
4. Click **Add Child** and configure the **City**. Click **Add**.





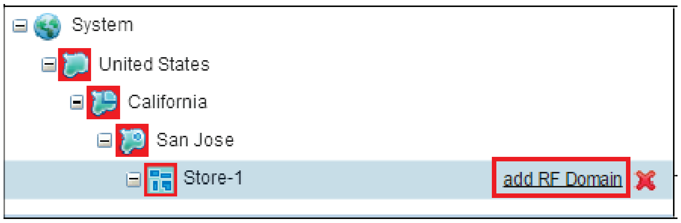
Name: San Jose *
Type: City

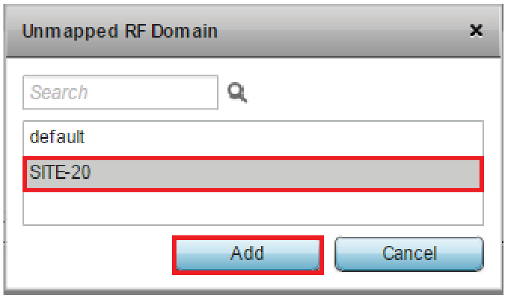
5. Click **Add Child** and configure the **Campus Name**. Click **Add**.



Name: Store-1 *
Type: Campus

6. Click **Add RF Domain** and select the RF-Domain from the list of RF Domains that are yet unmapped. Click **Add**.

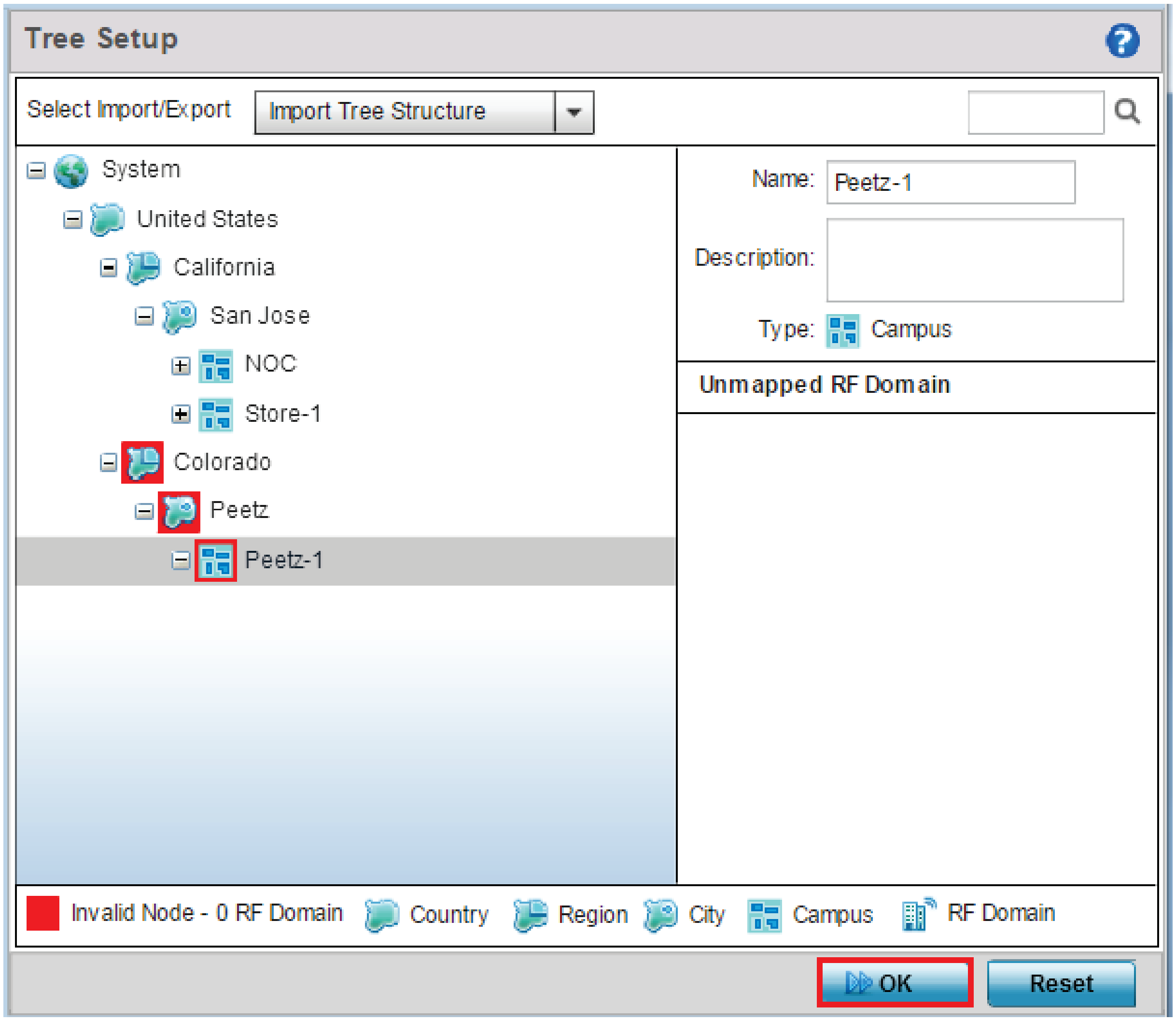




7. Complete the Tree Setup that best reflects your deployment. Click **OK**. Then click **Commit and Save**.

Note

Click **OK** followed by **Commit and Save**, otherwise the tree setup configuration will be lost.



Tree Setup

Select Import/Export: Import Tree Structure

- System
  - United States
    - California
      - San Jose
        - NOC
        - Store-1
    - Colorado
      - Peetz
        - Peetz-1

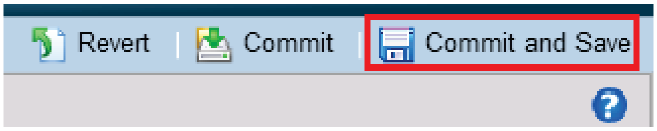
Name: Peetz-1

Description:

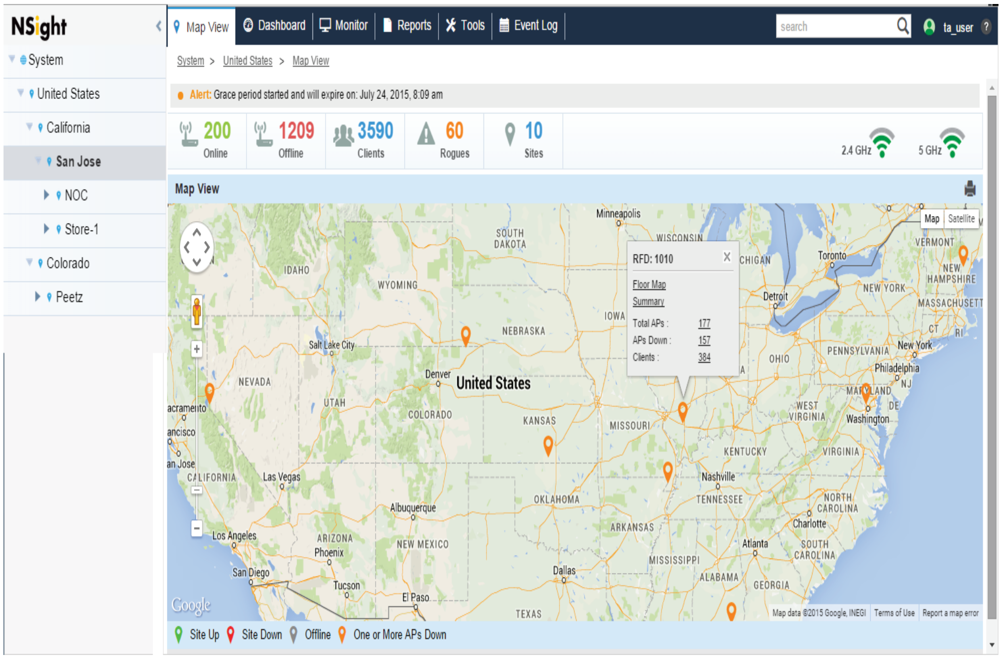
Type: Campus

Unmapped RF Domain

🟥 Invalid Node - 0 RF Domain | Country | Region | City | Campus | RF Domain



8. The tree hierarchy will now be available across the various screens – the Dashboard, Statistics on the WiNG UI and also on the NSight UI.



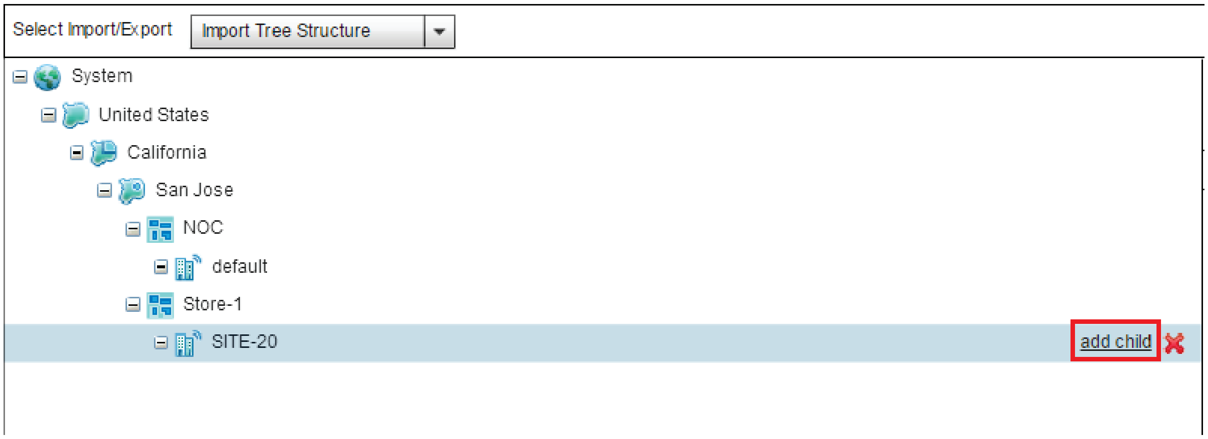
Alert: Grace period started and will expire on: July 24, 2015, 8:09 am

200 Online | 1209 Offline | 3590 Clients | 60 Rogues | 10 Sites

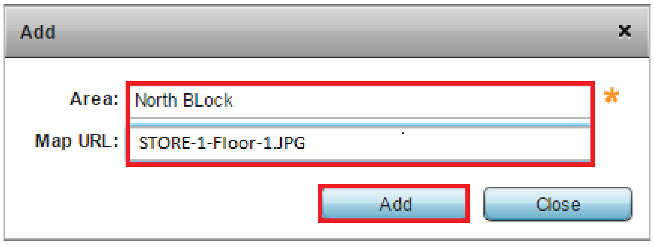
RFD: 1010
Floor Map
Summary
Total APs : 177
APs Down : 157
Clients : 384

9. A Floor should be added to the RF-Domains and APs should be assigned to each floor. This will also be used when creating floor maps for heat-maps in both WiNG and NSight.

   Click Add Child. Add the Area and floor map for the floor. The floor map file should be placed in the folder `flash:/floormaps/` in JPEG or PNG format. Click **Add**.



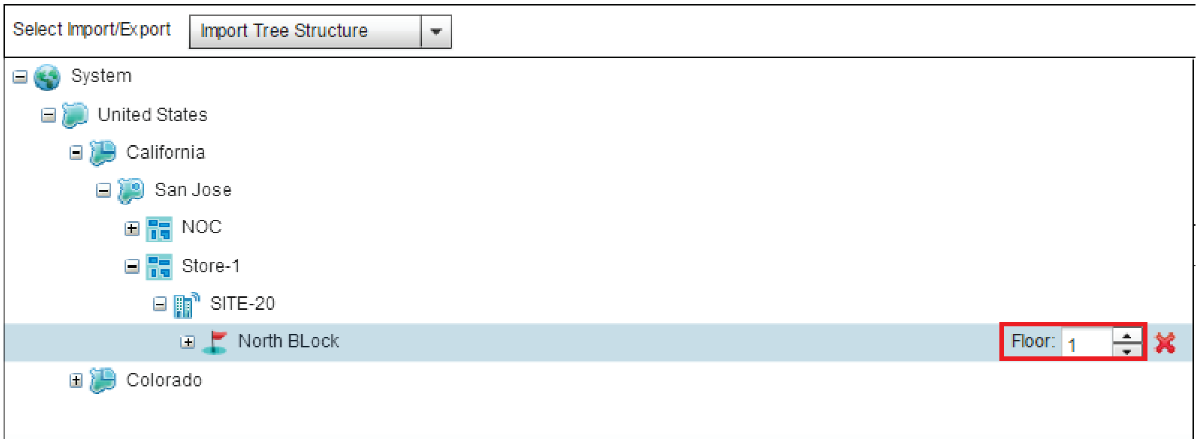
Select Import/Export: Import Tree Structure



Area: North BLock

Map URL: STORE-1-Floor-1.JPG

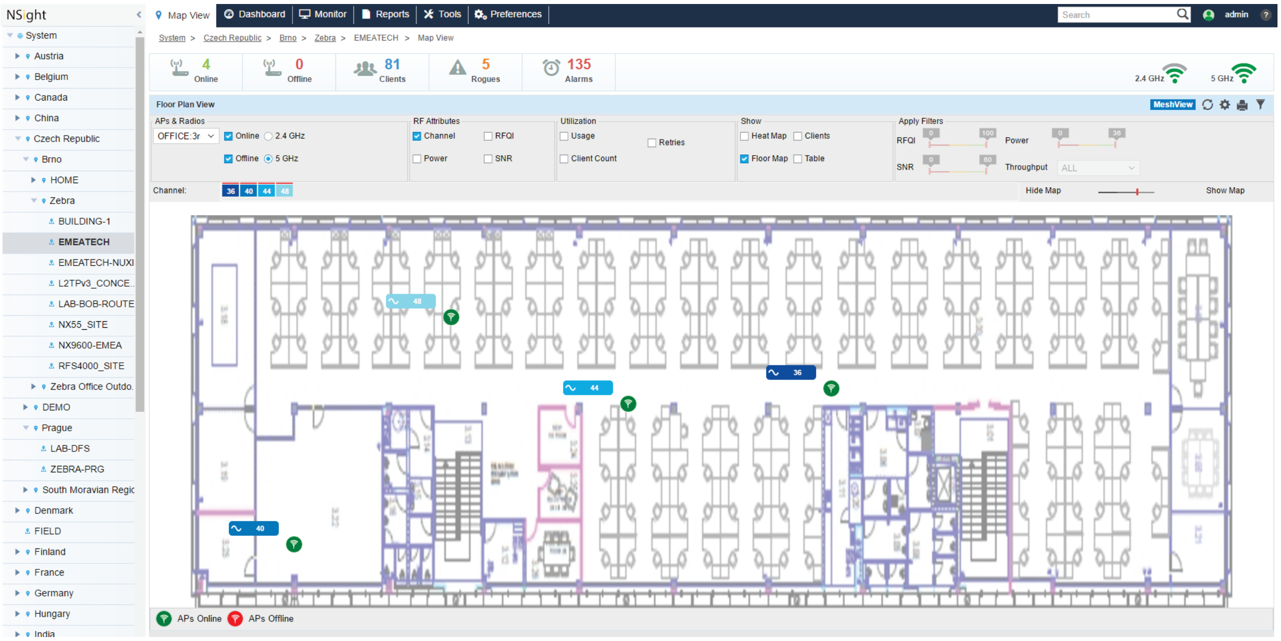
10. Add the number of Floors. Click **Commit and Save**.



Select Import/Export: Import Tree Structure

- System
  - United States
    - California
      - San Jose
        - NOC
        - Store-1
          - SITE-20
            - North BLock — Floor: 1
    - Colorado

11. Move Access points on to the floor using drag & drop on NSight UI. Navigate to **Map View** -> **Select RF-Domain** -> **Select Area: Floor:**



System > Czech Republic > Brno > Zebra > EMEATECH > Map View

- System
  - Austria
  - Belgium
  - Canada
  - China
  - Czech Republic
    - Brno
      - HOME
      - Zebra
        - BUILDING-1
        - **EMEATECH**
        - EMEATECH-NUXI
        - L2TPv3_CONCE..
        - LAB-BOB-ROUTE
        - NX55_SITE
        - NX9600-EMEA
        - RFS4000_SITE
      - Zebra Office Outdo.
    - DEMO
    - Prague
      - LAB-DFS
      - ZEBRA-PRG
    - South Moravian Regic
  - Denmark
  - FIELD
  - Finland
  - France
  - Germany
  - Hungary
  - India

4 Online | 0 Offline | 81 Clients | 5 Rogues | 135 Alarms | 2.4 GHz | 5 GHz

Floor Plan View

APs & Radios: OFFICE:3r | ☑ Online | ○ 2.4 GHz | ☑ Offline | ● 5 GHz

RF Attributes: ☑ Channel | □ RFQI | □ Power | □ SNR

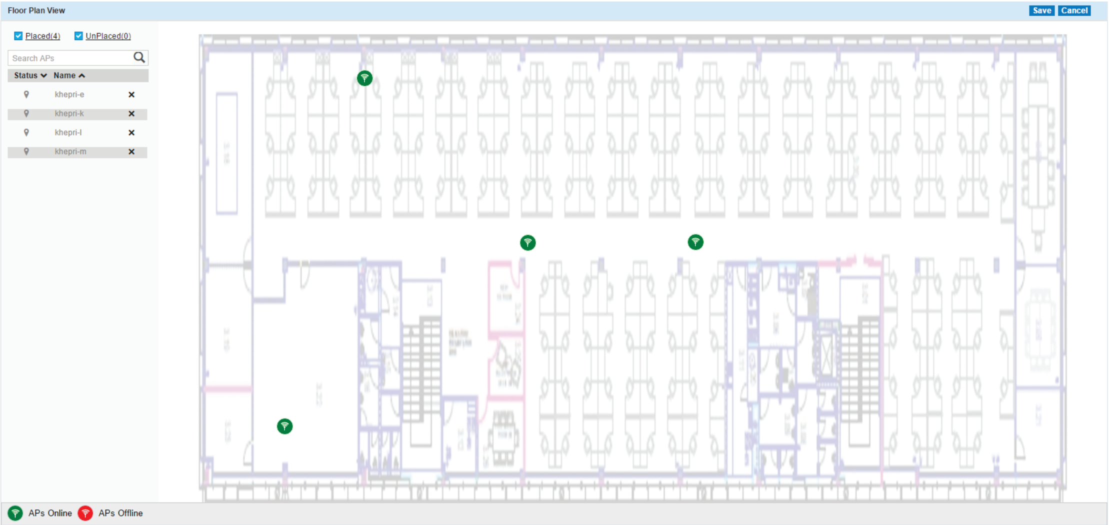
Utilization: □ Usage | □ Retries | □ Client Count

Show: □ Heat Map | □ Clients | ☑ Floor Map | □ Table

Apply Filters: RFQI 0–100 | Power 0–38 | SNR 0–60 | Throughput ALL

Channel: 36 40 44 48

● APs Online ● APs Offline



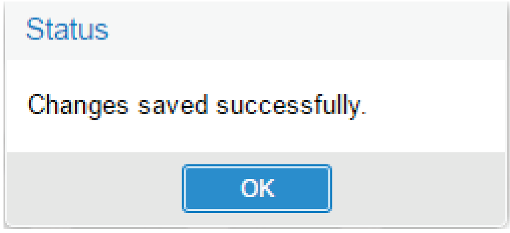
Floor Plan View

☑ Placed(4) ☑ UnPlaced(0)

Search APs

Status	Name	
⚲	khepri-e	×
⚲	khepri-k	×
⚲	khepri-l	×
⚲	khepri-m	×

● APs Online ● APs Offline



Status

Changes saved successfully.

12. **Standalone NSight ONLY**: Copy floorplans image files onto the flash:/floorplans/ directory of the NSight server. Keep the filename exactly the samWe as specified in WiNG configuration

    Example: filename configured for 1st Floor on RF-Domain “Store-1” is “store-1-floor1.jpg”. This file with the same filename must be loaded onto NSight server into flash:/floorplans/ folder.

```
NSIGHT-STANDALONE-1#dir flash:/floorplans/
Directory of flash:/floorplans/
  -rw-    258852    Tue Nov 24 23:39:19 2015   Alphanet2-SF.JPG
  -rw-    258852    Tue Nov 24 23:39:19 2015   Alphanet1-SF.JPG
  -rw-    258852    Tue Nov 24 23:39:19 2015   Alphanet-SF.JPG
  -rw-    143610    Thu Nov 26 12:57:35 2015   store-1-floor1.jpg
```

Online / Offline Device State Detection

Device state detection is part of NSight server functionality. The detection logic is based on observing wired port statistics reported from remote devices. In NSight deployments every RF Domain manager reports statistics for all devices in the RF Domain. After the statistics are posted to the database the primary NSight server uses them to detect online/offline state of all devices in RF Domain.

Online/offline state is distinct from adopted/un-adopted state. In vast majority of cases a device is either adopted and online or un-adopted and offline. However, in few cases the two can diverge, specifically:

a. Devices adopted but belonging to RF Domain that does not have correct NSight policy might appear adopted but offline (adopter has correct NSight policy and reports adoption and configuration tree to the NSight server but RF Domain Manager does not have correct NSight policy and fails to report statistics to the NSight server).
b. Devices deleted from the configuration and prevented from re-adoption by auto-provisioning policy will appear online and unadopted.

Online/Offline device detection is based on wired ports statistics received from remote Access Points or Controllers (each device MAC address will have wired statistics associated with it):

NSight servers runs a device online detection process once every 3 minutes, therefore showing a device as offline or online might not be immediate. For offline device detection there is an additional grace period that allows 2 missing statistics updates rounded up to the next 3 minute detection cycle before marking the device as offline. For example, with stats report interval of 30 seconds it might take up to 6 minutes to detect a device being offline.

Two offline states are possible for a device that was detected to be offline - offline (in the configuration and offline) and deleted (deleted from the configuration and offline). This is selected based on the last known configuration state received from the WiNG controller.

Location Based Access Control – Multi Tenancy

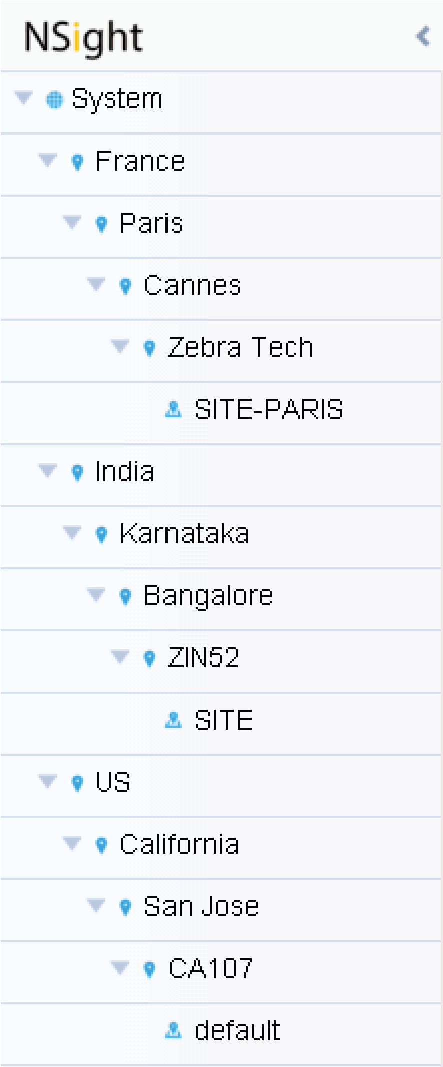
By default, a user logging into NSight UI will have access to all RF domains and locations. However, in certain deployments, it is desirable to provide management access to specific rf-domains and restrict all other access.

To configure Location based access, the user is given access to a specific RF-Domain or a certain level in the tree hierarchy, like for example a Country or Campus. If the access is given to a location in the hierarchy tree, the user will get access to all the RF Domains that fall under that location.

There are three options to achieve this functionality:

1. Configure allowed-location on the NSight and associate it to management users.

   As an example below let’s assume following tree structure:



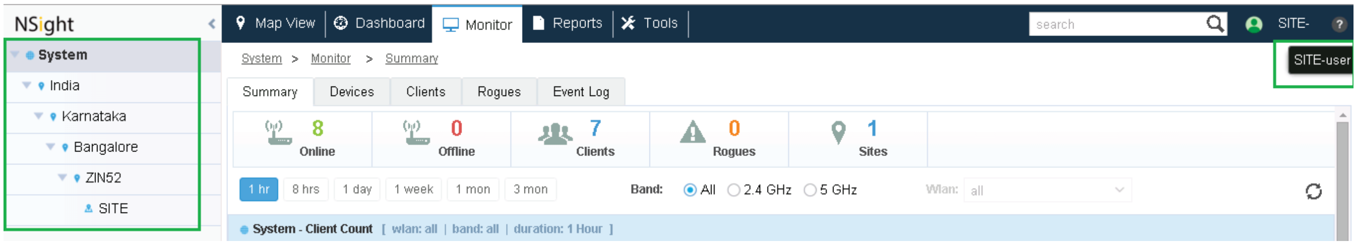
Allowed-location alias under management policy can be used to allow access only to specific RF Domain(s).

```
PRIMARY(config)#management-policy default
PRIMARY(config-management-policy-default)#allowed-locations India ?
  locations  List of locations

PRIMARY(config-management-policy-default)#allowed-locations India locations ?
  LINE  NONE - do not allow any locations
        ALL  - allow all locations
        list locations, either a path - /US/California or individual rf domain
        - site-0123

PRIMARY(config-management-policy-default)#allowed-locations India locations SITE
PRIMARY(config-management-policy-default)#user India-user password test role superuser access all allowed-
locations India
PRIMARY(config-management-policy-default)#commit write
```

Now when this new user logs into the NSight UI with 'India-user' username, she will have access only to SITE rf-domain and all other RF Domains and locations will not be visible:



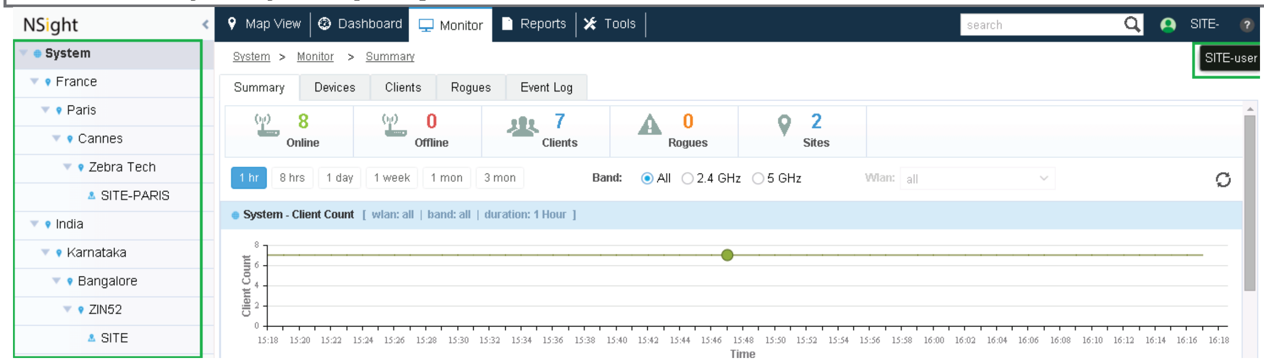
Allowed-location can be configured to provide access to certain Tree item, i.e. a Country, which may include multiple RF Domains:

```
PRIMARY(config-management-policy-default)#allowed-locations India locations ?
  LINE  NONE - do not allow any locations
        ALL  - allow all locations
        list locations, either a path - /US/California or individual rf domain
        - site-0123

PRIMARY(config-management-policy-default)#allowed-locations France locations /France/
```

Multiple sites and locations can be attached to a particular allowed-locations:

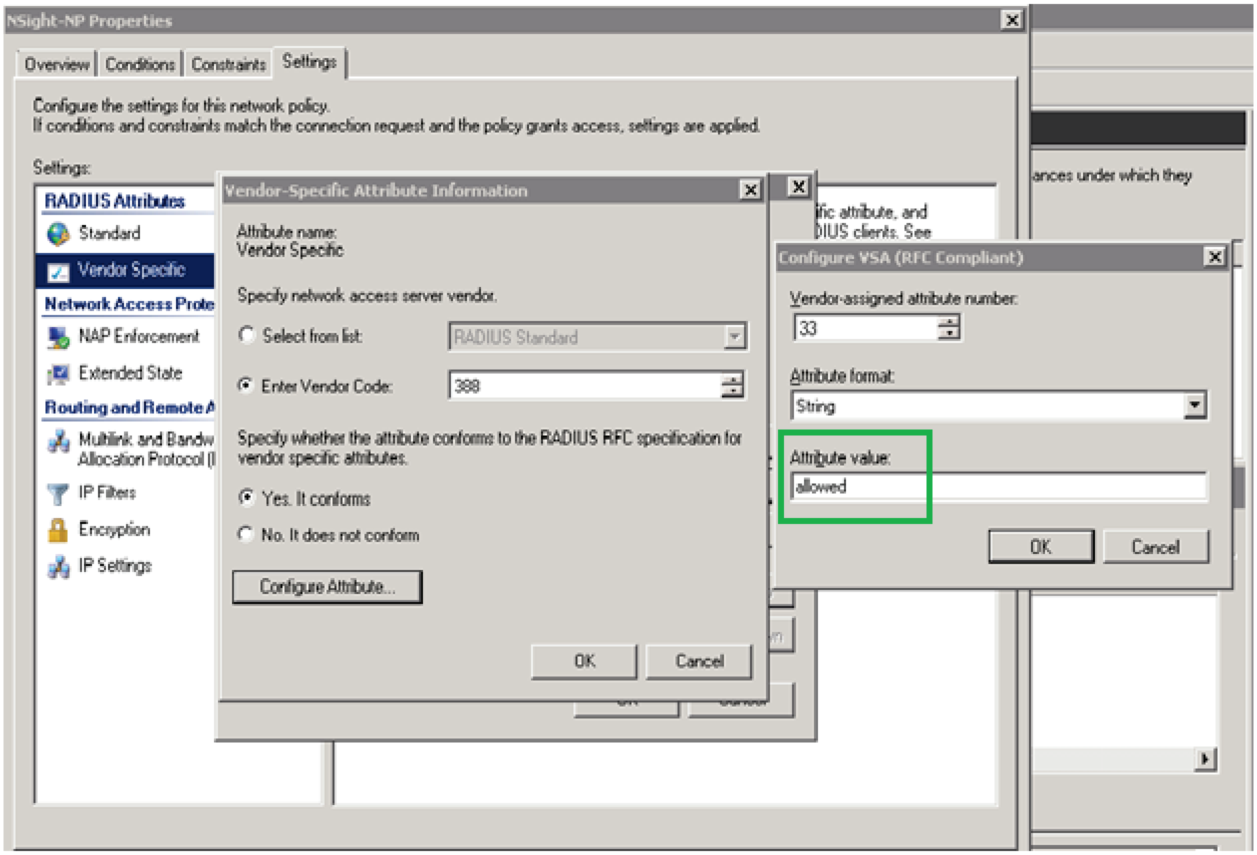
```
PRIMARY(config-management-policy-default)#allowed-locations IndiaPlusFrance locations SITE /France/
PRIMARY(config-management-policy-default)#user India-user password test role superuser access all allowed-
locations IndiaPlusFrance
PRIMARY(config-management-policy-default)#commit write
```



2. Dynamically select allowed-location based on management user authentication using RADIUS.

If a management user is authenticated using RADIUS, **`allowed-location`** name can be sent via RADIUS using Vendor Specific Attribute (VSA) with **`attribute value`** 33 and **`Vendor code`** 388 as a **`string`**.

VSA can be configured on the RADIUS Server:



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Attribute name:
Vendor Specific

Specify network access server vendor.

○ Select from list: RADIUS Standard

● Enter Vendor Code: 388

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

● Yes. It conforms

○ No. It does not conform

Vendor-assigned attribute number: 33

Attribute format: String

Attribute value: allowed

In this example “allowed” is the name of the allowed-location alias configured to allow access to specific rf-domain(s).

```
NSIGHT-PRIMARY(config-management-policy-default)#allowed-locations allowed locations /US/California/
```

User needs to configure the allowed-location alias under management before it can be applied via RADIUS into the NSight UI.

Note

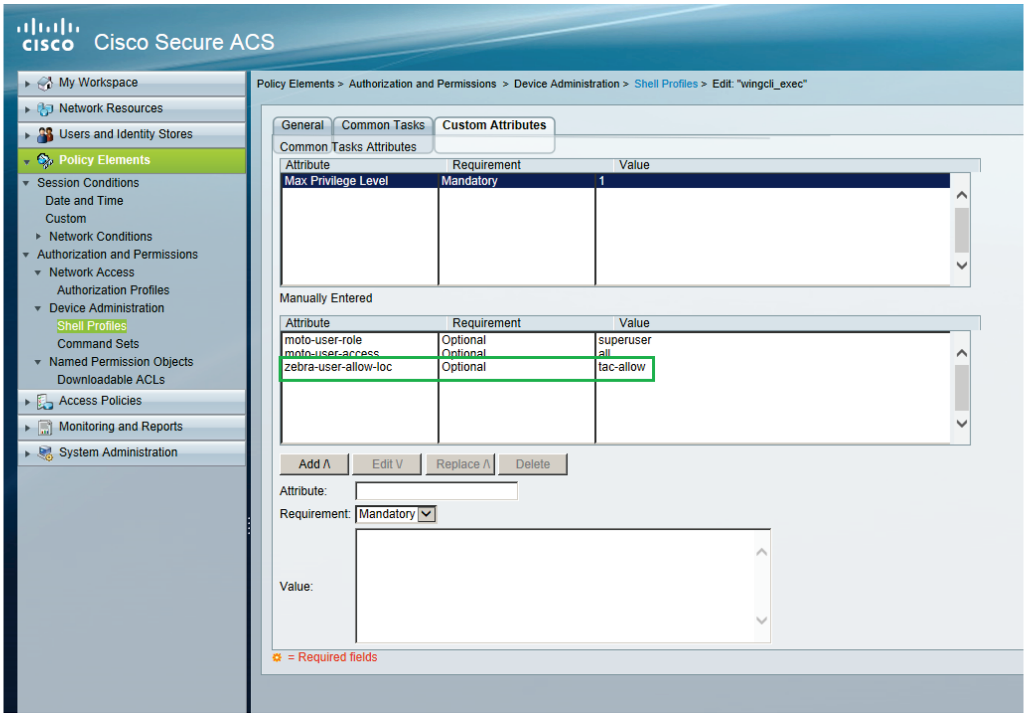
If there is no allowed-locations attribute in the RADIUS Access-Accept by default all locations will be allowed.

If the user has configured a VSA attribute value which doesn’t exist on the device management policy access to all locations will be denied.

3. Dynamically select allowed-location based on management user authentication using TACACS.

Similar to RADIUS, during authentication of management user using TACACS, allowed-location name can be optionally provided using the Custom Attribute. Attribute name is **`zebra-user-allow-loc`**. Value can be a string which is the configured allowed-location name on the NSight server.

Custom Attribute can be configured on TACACS to specify allowed-location attribute name:



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "wingcli_exec"

Attribute	Requirement	Value
Max Privilege Level	Mandatory	1

Manually Entered

Attribute	Requirement	Value
moto-user-role	Optional	superuser
moto-user-access	Optional	all
zebra-user-allow-loc	Optional	tac-allow

Attribute:

Requirement: Mandatory

Value:

In this example 'tac-allow' is the name of the allowed-location configured to allow access to specific RF-domain(s).

```
NSIGHT-PRIMARY(config-management-policy-default)#allowed-locations tac-allow locations /US/California/
```

Same as with RADIUS allowed-locations alias must be already configured on the NSight server before logging into the NSight UI.

If the TACACS authentication policy is not configured with custom attribute **zebra-user-allow-loc**, by default we allow all locations.

If the user has configured a custom attribute with allowed-locations name, which doesn't exist on the NSight server access will be denied to all locations.

Note

Please note that in all cases access restriction is enforced on the NSight UI only. If the user logs on to the WiNG5 console, the user will have access in accordance to his role. But he can view the statistics on the WiNG UI for any location.

NSight Statistics Update Intervals

NSight database is summarizing older statistics into aggregated (averaged) records to optimize storage usage and prevent database growing to unmanageable size. All periodic records beyond fixed time period are summarized into one record by making an average of them.

WiNG 5.8.2.0 release added an option to control and tweak how frequently and for how long data will be aggregated for each statistics bucket, i.e. ability to configure granularity and duration for some statistics buckets to optimize storage usage, while still proving the average for any given time period.

Main terms&definitions:

- Statistics Bucket – Statistics Bucket is database collection that holds statistics data on per RF Domain basis

- Granularity - the interval at which records are posted into bucket.
- Duration – the time for which records are maintained in a particular bucket. E.g. for RAW bucket records are maintained for specified 8 hours (default), after which the records are purged.

Statistics Buckets	RAW data	10 Min data	Hourly data	Daily data
Granularity	30 sec – 10 min	10 min	1 hour	24 hours
Duration	1 – 8 hours	1 – 168 hours	1 – 2160 hours	24 – 26280 hours
Duration Defaults	8 hours	24 hours	7 days	1 year

Granularity configuration options:

In addition to global nsight update interval, 5.8.2 adds an option to define update interval for specific type of statistics, like AVC and Wireless Client statistics:

	Configuration options	Default interval
General update interval	30/60/120/300/600 seconds	60 seconds
AVC stats	30/60/120/300/600 seconds	300 seconds
Wireless Client stats	30/60/120/300/600 seconds	300 seconds
Max # of Apps per MU reported	1 - 1000	10 Applications per MU

Configuration

Caution

Configuration of update interval is disruptive operation, which will result in data loss. It is recommended to set these values based on scalability requirements. Typically, these should be left untouched.

1. Stop NSight service on all members of replica set:

```
NSIGHT-PRIMARY#conf
Enter configuration commands, one per line.  End with CNTL/Z.
NSIGHT-PRIMARY(config)#nsight-policy STANDALONE
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#no enable
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#commit write
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#end
```

2. Remove all files in the database – this will cause a reboot and data loss:

```
NSIGHT-PRIMARY#service database remove-all-files

*************************************  WARNING  **************************************
** Execution of this command will erase all files related to the database server. **
** This device will reload after execution.                                        **
**************************************************************************************
Are you sure you want to remove all database related files? (y/n): y
```

3. After reboot reconfigure new NSight update intervals to a desired value (see appendix for scalability reference):

```
NSIGHT-PRIMARY#self
Enter configuration commands, one per line.  End with CNTL/Z.

NSIGHT-PRIMARY(config-device-02-52-C5-FC-89-75)#nsight database statistics ?
  avc-update-interval               NSight database AVC statistics update
                                    periodicity in seconds
  max-apps-per-mu                   NSight database max mu-apps to be posted
                                    in an update-interval (default 10)
  update-interval                   NSight database statistics update
                                    periodicity in seconds
  wireless-clients-update-interval  NSight database wireless clients
                                    statistics update periodicity in seconds

================================================================================
AVC update interval
================================================================================
nsight database statistics avc-update-interval ?

  120  2 minutes
  30   30 seconds
  300  5 minutes
  60   1 minute
  600  10 minutes

================================================================================
Max number of applications per client
================================================================================

nsight database statistics max-apps-per-client ?

  <1-1000>  Number for apps to be posted

================================================================================
Statistics Update Interval
================================================================================

nsight database statistics update-interval ?

  120  2 minutes
  30   30 seconds
  300  5 minutes
  60   1 minute
  600  10 minutes

================================================================================
Wireless client statistics update interval
================================================================================

nsight database statistics wireless-clients-update-interval ?

  120  2 minutes
  30   30 seconds
  300  5 minutes
  60   1 minute
  600  10 minutes

================================================================================
Edit Duration values
================================================================================

nsight database summary duration ?
  <1-24>  Bucket 1 duration in hours (min 1 hour, max 24 hours, default 8
          hours)

nsight database summary duration 8 ?
  <1-168>  Bucket 2 duration in hours (min 1 hour, max 168 hours (7 days),
           default 24 hours)

nsight database summary duration 8 24 ?
  <1-2160>  Bucket 3 duration in hours (min 1 hour, max 2160 hours (90 days),
            default 7 days)

nsight database summary duration 8 24 168 ?
  <24-26280>  Bucket 4 duration in hours (min 24 hours (1 day), max 26280
              hours (3 years), default 365 days)
```

4. Re-enable NSight

```
NSIGHT-PRIMARY#conf
Enter configuration commands, one per line.  End with CNTL/Z.
NSIGHT-PRIMARY(config)#nsight-policy STANDALONE
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#enable
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#commit write
NSIGHT-PRIMARY(config-nsight-policy-STANDALONE)#end
```

Note

It may take up to 5 minutes for the RF-Domain managers to get the updated value of nsight statistics update interval.

NSight Guest Users

In a typical guest access environment customers may observe thousands of unique clients every day. By default NSight server will keep historical data for each wireless client for up to 180 days, which for guest networks may become burdensome to keep thousands if not millions of unique MAC addresses in the database which may have visited the customer only once or twice. To address this potential problem it is recommended to disable Guest Access Wireless LANs to keep clients in the NSight database for a long time. For those clients there would be a separate timer (8 hours by default) which will determine for how long each client will stay in the database. Configuration is CLI only:

```
 !
wlan Z-Guest
 ssid Z-Guest
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type mac
 radio-resource-measurement
 use aaa-policy ONBOARD
 use captive-portal REGISTRATION
 captive-portal-enforcement fall-back
 registration device-OTP group-name GUESTS expiry-time 4320 agreement-refresh 1440
 registration external host 140.101.4.17
 use ip-access-list out BROADCAST-MULTICAST-CONTROL
 use mac-access-list out PERMIT-ARP-AND-IPv4
 no nsight client-history
 !
```

Additionally NSight History Time To Live values can be adjusted at the NSight Server policy to reduce or increase the period for how long to store the data.

```
 !
nsight-policy STANDALONE-SERVER
 enable
 nsight-server standalone
 history-ttl devices 180
 history-ttl clients 180
 history-ttl guest-clients 8
 event-history-size low
 !
```

Devices – adopted APs or Site Controllers. Set in days.

Clients – Wireless Clients when “nsight client-history” is enabled under WLAN - default. Set in days.

Guest-Clients – Wireless Clients when “nsight client-history” is disabled under WLAN. Set it hours.

Event-History Size – Low (up to 500K events), Medium (up to 5M events), High (up to 10M events).

Database Management and Monitoring

Enable Database Events

It is recommended to enable the Database events in the Event System policy so that attention is drawn towards any error condition in the NSight Database. They will be generated by default on the event log on the console, but the user might want to receive them in some other manner, like Email or SNMP.

Database-election-fail requires manual intervention to select primary database node.

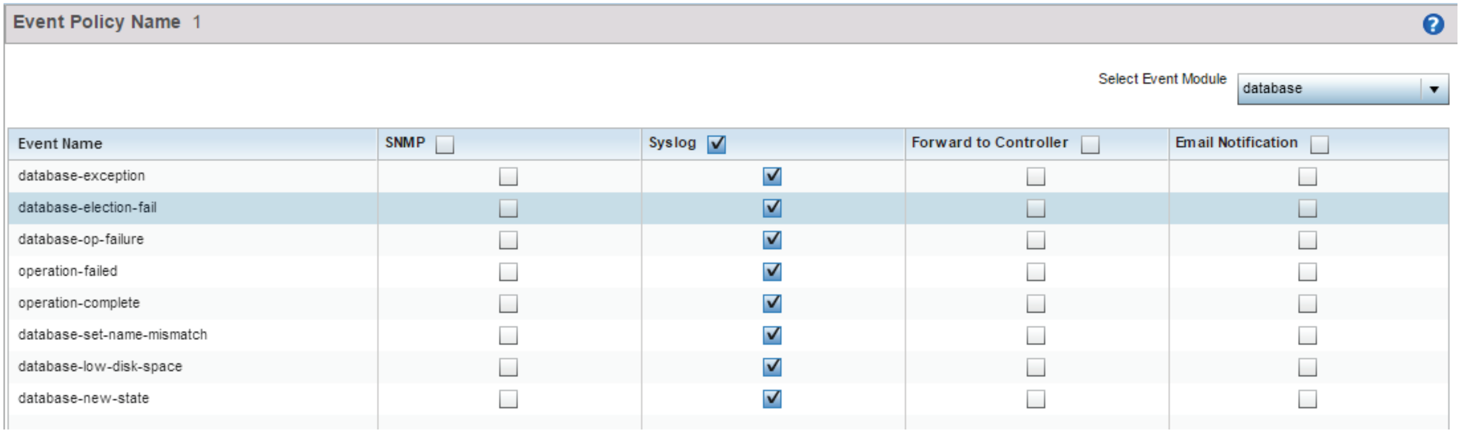
Database-exception indicates that the database is corrupted and needs manual intervention.

Operation failed and operation complete are generated in response to the success or failure of database backup and restore.

List of all database related events:

Event	Description
DATABASE-4-DATABASE_SET_NAME_MISMATCH: MongoDB replica set name mismatch on host [host]	Identified host do not have a database-policy applied. Check the configuration on the identified hosts.
DATABASE-5-DATABASE_NEW_STATE: Database server is now RS_PRIMARY|RS_SECONDARY	Triggered when the role of a replica member changes.
DATABASE-4-DATABASE_OP_FAILURE: <Message>	Triggered when a database operation fails, e.g. backup or restore.
DATABASE-6-DATABASE_OPERATION_COMPLETE: scheduled backup for database [database] success full failed	Check flash:/log/mongod.log file for details.
DATABASE-4-DATABASE_LOW_DISK_SPACE: Available disk space [space] is below threshold [threshold]	Triggered when a scheduled backup has completed successfully or failed.
DATABASE-1-DATABASE_STORAGE_MISMATCH: Database server did not start because data files are incompatible with the current storage engine	Triggered when available disk space on the database storage volume falls below the configured low-disk-space-threshold.

Database Events Configuration:



Event Policy Name 1

Select Event Module: database

Event Name	SNMP □	Syslog ☑	Forward to Controller □	Email Notification □
database-exception	□	☑	□	□
database-election-fail	□	☑	□	□
database-op-failure	□	☑	□	□
operation-failed	□	☑	□	□
operation-complete	□	☑	□	□
database-set-name-mismatch	□	☑	□	□
database-low-disk-space	□	☑	□	□
database-new-state	□	☑	□	□

```
NX(config-event-system-policy-1)#show context include-factory | grep database
 event database database-exception syslog default snmp default forward-to-switch default email default
 event database database-election-fail syslog default snmp default forward-to-switch default email default
 event database database-op-failure syslog default snmp default forward-to-switch default email default
 event database operation-failed syslog default snmp default forward-to-switch default email default
 event database operation-complete syslog default snmp default forward-to-switch default email default
 event database database-low-disk-space syslog default snmp default forward-to-switch default email default
 event database database-set-name-mismatch syslog default snmp default forward-to-switch default email
default
 event database database-new-state syslog default snmp default forward-to-switch default email default
NX(config-profile-NX9600)#show context include-factory | grep disk-space
database low-disk-space-threshold 30
```

Database Backup and Restore

The NSight Database can be exported to an external storage for backup, either on-demand or scheduled at specified time intervals. Customers are encouraged to make backups regularly or at least before any system changes or firmware upgrades.

Database Export

Backup the Database files on FTP server with specified IP address, username and password

On-demand database backup

```
PRIMARY#database-backup database nsight <destination-URL>
// The Destination URL can be specified using FTP or SFTP
```

Scheduled Database Backup

The database backup can be scheduled for a later time. The period of recurrence can be specified. The configuration should be done in the device context.

Scheduled database backup configuration (reoccurrence time in hours):

```
PRIMARY#self
PRIMARY(config-device-06-71-B1-5D-77-51)#database backup database nsight <destination URL> start-date
<MM/DD/YYYY> start-time <HH:MM> reoccurrence <time in hours>
// The Destination URL can be specified using FTP or SFTP
// reoccurrence specified the time period after which the backup will be repeated
```

Database Restore from Backup

Database restore from backup:

```
PRIMARY#database-restore database nsight <source-URL>
// The Source URL can be specified using FTP or SFTP
```

Best Practices on Database Management

It is important to note the points below to prevent any database corruption

1. Do not restart the NSight server when Database backup or restore is in progress.
2. Enable all database related events to monitor database health and operations status.
3. Make regular database backups.
4. Deploy replica set members to ensure high availability and data redundancy.

Database Service Commands

These commands should only be used as directed by support staff or as in documented procedures outlined in this guide.

Command	Description
`service database drop (nsight|captive-portal) collection (WORD)`	Drops the specified collection from the selected database.
`service database remove-all-files`	Removes all files related to the database server. Requires the database server to be stopped. Reloads the device after execution.
`service database replica-set (add|delete) member (A.B.C.D | WORD)`	Allows direct manipulation of the replica-set members.
`service database server (start|stop|restart)`	Starts, stops or restarts the database server.
`service database use-secondary-storage (VX9000 only)`	The VX9000 default partition table is limited to a partitions with a maximum size of 2 terabytes. This command provides support for an additional virtual disk with a partition table format supporting partition sizes in excess of 2 terabytes. This command should be used only as documented in the “Using secondary storage” section of this guide. Refer to section 3.4 for details.

VX9000 Secondary Storage Option

The current VX9000 has a disk size limitation on the default disk of 2 Terabytes. Should this not be of a sufficient size for the database server storage, the VX9000 can use a second virtual disk. When using a second disk, the VX9000 can support disks with sizes greater than 2 Terabytes.

Note
Consult the Virtual Hosting platform's documentation to determine how to provision an additional virtual disk for the VX9000 guest installation. Once this additional disk has been provisioned and the VX9000 guest restarted, secondary storage can be enabled.

Warning

Enabling secondary storage does not copy data files to the new location.

Careful consideration should be given when considering enabling secondary storage. The best time to enable it is immediately after provisioning the guest instance, before enabling NSight or Captive Portal.

If there is a requirement to enable secondary storage after the initial provisioning of the VX9000 guest instance, it is advised that backups of the databases (NSight and/or Captive-portal) be taken before enabling secondary storage. After secondary storage is enabled, the database can be restored.

Alternatively, if the VX9000 instance is a member of a replica-set and is not the primary, the database server will perform a full data sync after it is restarted using the new storage disk.

To enable secondary storage, execute the following command:

```
PRIMARY#service database use-secondary-storage

************************************  WARNING  *************************************
** Execution of this command will configure this device to store the database     **
** files on a secondary drive.  This device will reload after execution.          **
** NOTE: Current database files will be erased.                                   **
************************************************************************************
Are you sure you want to proceed? (y/n): y
Enabling secondary storage on sdb.................complete.
Using sdb for secondary database storage
PRIMARY#
```

VM Snapshots as a recovery mechanism

VX9000 is the only platform that can scale beyond 10,000 devices in NSight.

When VX9000 is running a Database Server it is recommended to utilize hypervisor VM Snapshot mechanism for recovery purposes.

Recovery mechanism will be required in the following scenarios:

- NSight server on VX has stopped responding or not booting up.
- NSight server database has got corrupted.
- NSight server has been upgraded recently and needs to be restored to a previous point due to unforeseen issues.

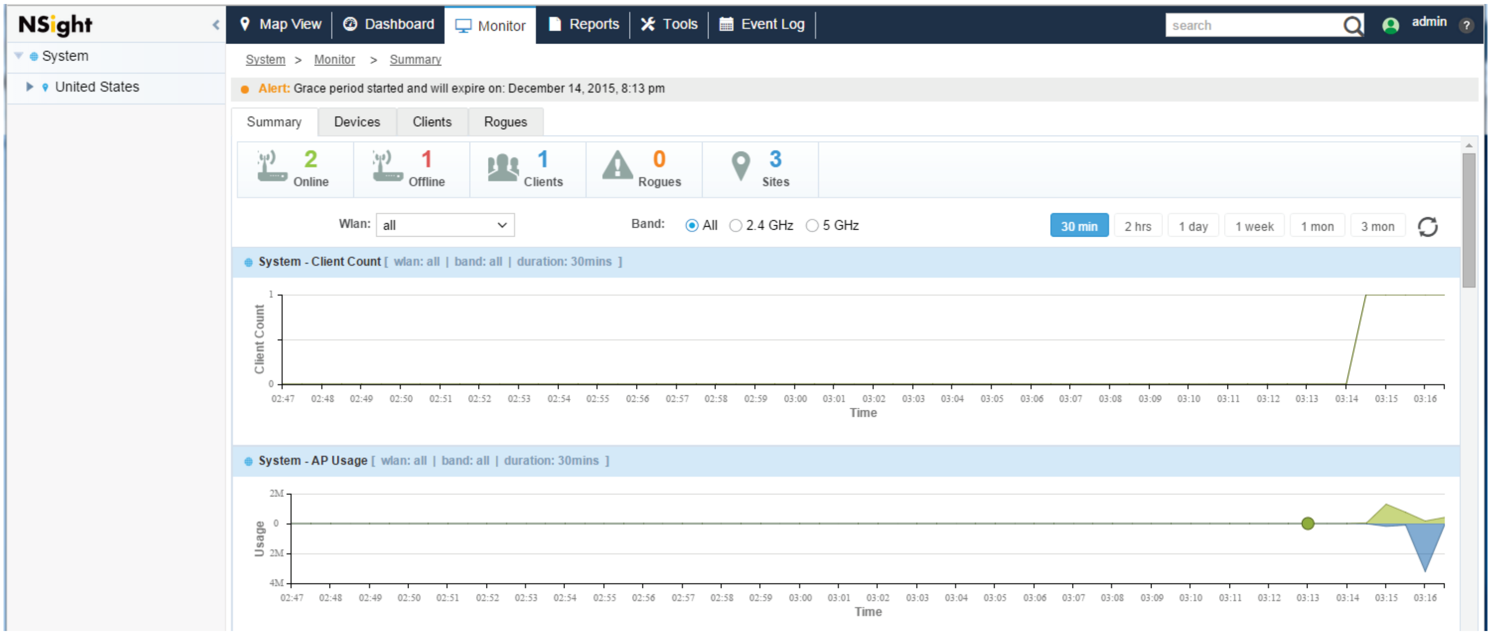
Recommendations:

- Snapshots should be take on a healthy NSight Sever
- Create a snap shot every week or 3 days and discard the old snapshot once the new snap shot is available.
- Take a snapshot before any upgrades of NSight server.

Verification

NSight UI

Login to the NSight UI. **Monitor** -> **Summary** screen is the default view. If the license is installed and the configuration is complete, user can start seeing bandwidth usage and clients count on the **Monitor** -> **Summary** screen.



Alert: Grace period started and will expire on: December 14, 2015, 8:13 pm

Statistics

NSight Process Status

```
NSIGHT-PRIMARY#show nsight status
Nsight is enabled
 Nsight report and aggregation daemon is running
 Nsight alarm daemon is running
 Nsight server daemon is running
 Database server is local
 Database server is reachable
```

Database Statistics

Please use the command below for getting the database statistics:

```
NSIGHT-PRIMARY#show database statistics
--------------------------------------------------------------------------------
       DATABASE         STORAGE SIZE   DATA SIZE     INDEX SIZE      DISK FREE
--------------------------------------------------------------------------------
  nsight               210.0M          770.0M       120.4M         138.0G
  captive_portal       4k              0            24k            138.0G
  nsightcache          144k            79.6k        284k           138.0G
--------------------------------------------------------------------------------
```

Database Status

The command below indicates that status of the Database and database state (primary, secondary or arbiter).

```
NSIGHT-PRIMARY#show database status
--------------------------------------------------------------------------------
          MEMBER                STATE                        ONLINE TIME
--------------------------------------------------------------------------------
  172.31.0.49*             PRIMARY               7 hours 56 min 2 sec
  172.31.2.248             SECONDARY             7 hours 55 min 38 sec
  172.31.5.121             ARBITER               7 hours 55 min 57 sec
--------------------------------------------------------------------------------
[*] indicates this device.
```

Debugging

(should be run on the NSight server, required logging to be enabled and set to debug level)

Debug Module	Description
`debug` **`nsightd`**	NSight Reporting daemon debug
`debug nsight` **`alarm`** `level <level*>`	NSight Alarm related debugs
`debug nsight` **`chart`** `level <level*>`	NSight chart related debugs
`debug nsight` **`client`** `level <level*>`	NSight wireless client related debugs
`debug nsight` **`dashboard`** `level <level*>`	NSight custom dashboard related debugs
`debug nsight` **`device`** `level <level*>`	NSight device (AP/Controller) related debugs
`debug nsight` **`eventlog`** `level <level*>`	NSight Event system related debugs
`debug nsight` **`kms`** `level <level*>`	NSight Key Metric System related debugs (Number of Online/Offline devices, clients, rogues, etc)
`debug nsight` **`location`** `level <level*>`	NSight Location related debugs (AP placements on floor map)
`debug nsight` **`monitor`** `level <level*>`	NSight Monitor View related debugs (AP placements on floor map)
`debug nsight` **`rfdomain`** `level <level*>`	NSight RF Domain Manager related debugs (all POST from each RFD for each database collection will be seen here)
`debug nsight` **`server`** `level <level*>`	NSight core process debug
`debug nsight` **`smartrf`** `level <level*>`	NSight SmartRF related debugs
`debug nsight` **`summarization`** `level <level*>`	NSight Database Aggregation related debugs

Level	Description
error	Only errors
info	Errors, warnings, as well as informational level traces (default)
warn	Errors as well as warning level traces
debug	Errors, warnings, info and basic debug trace messages for the selected modules
debug2	Errors, warnings, info and two levels of debug trace messages for the selected modules
debug3	Errors, warnings, info and three levels of debug trace messages for the selected modules
debug4	Errors, warnings, info and all levels of debug trace messages for the selected modules

Appendix

Supported Platforms

NSight is supported on the NX95XX, NX96XX and VX 9000 platforms in both standalone server and integrated WiNG+NSight modes

Scaling – NSight on Hardware Appliances

The scaling information below should be used to correctly design and implement a NSight deployment.

Controller Platform	Number of Access Points (max 1,000 RF Domains)	Stats Update Interval	AVC Update Interval	Wireless Client Update Interval
NX 95X0 / NX96XX	2,500	1 min	5 Min	5 Min
NX 95X0 / NX96XX	5,000	2 Min	5 Min	5 Min
NX 95X0 / NX96XX	10,000	5 Min	5 Min	5 Min

Scaling – NSight on Virtualized VX9000 Platform

# of APs or RF Domains	100	500 / 100	1000/200	2000/500	5000/1000	10000/500
CPU	8 core @2.5 GHz	12 core @2.5 GHz	18 core @2.7 GHz	24 core @2.7 GHz	24 core @2.7 GHz	24 core @2.7 GHz
Memory (DDR3-L or DDR4)	16 GB	32 GB	40 GB	64 GB	96 GB	128 GB
Storage / Config	500 GB RAID1+0	500 GB RAID1+0	500 GB RAID1+0	500 GB RAID1+0	2 TB RAID1+0 4 x 500 GB SSD (SLC)	5 TB RAID1+0 8 x 500 GB SSD (SLC)
IOPS	2,000 sustained writes	2,000 sustained writes	3,000 sustained writes	4,000 sustained writes	4,000 sustained writes	4,000 sustained writes

Capacity (APs / RF Domains / Clients)	10,000 / 1,000 / 100K	15,000 / 1,500 / 150K	20,000 / 2,000 / 300K	25,000 / 2,000 / 300K	30,000 / 2,000 / 300K	40,000 / 2,000 / 600K
CPU	24 core @2.5 GHz	24 core @2.5 GHz	32 core @2.5 GHz	32 core @2.6 GHz	32 core @2.6 GHz	32 core @2.6 GHz
Memory (DDR3-L or DDR4)	128 GB	128 GB	128 GB	128 GB	256 GB	256 GB
Storage / Config	500 GB RAID1+0	1 TB RAID1+0	2 TB RAID1+0 4 x 500 GB SSD (SLC)	2 TB RAID1+0 4 x 500 GB SSD (SLC)0	2 TB RAID1+0 4 x 500 GB SSD (SLC)	5 TB RAID1+0 8 x 500 GB SSD (SLC)
IOPS	3,000 sustained writes	4,000 sustained writes	4,000 sustained writes	4,000 sustained writes	4,000 sustained writes	8,000 sustained writes

Bandwidth Requirements

The APs and controllers exchange management traffic with each other. In distributed deployments, the APs may be connected to the Data Center using a variety of WAN technologies, like MPLS, xDSL, DOCSIS, 3G or 4G services. With the APs using Level 2 MINT Link for adoption to the controller, the bandwidth required for management traffic is typically 5-10 kbps per AP. Please check the How-To guide on Centralized deployment for more details.

The additional bandwidth when deploying NSight for reporting the statistics from each site to the NOC is less than 1kbps per AP.