

HiveManager Classic to XIQ Migration Guide

by Mike Rieben, SA – 2/4/2022

Overview:

Aerohive HiveManager Classic & HiveManager NG have been replaced by ExtremeCloud IQ (XIQ). This guide covers many aspects of the migration process. You start by documenting the existing system, addressing any licensing concerns, verifying device compatibility, backup and restoring a portion of the Classic system, configuring XIQ, and scheduling an outage to systematically migrate devices site by site. You control the outage impact. All the configuration is complete upfront without affecting the existing production network. This is a great opportunity to abandon old configurations and simplify your setup.

Target Audience: Technical

Prerequisites:

- Contact your Extreme Account Sales Team for any licensing assistance
 - You may email:
 - Americas: SAASTEAMAMER@extremenetworks.com
 - International: SAASTEAMINT@extremenetworks.com
- Access to HiveManager Classic (Cloud or On-prem) using a super admin account:
 - Must have the ability to delete devices from the system
 - If not, reach out to GTAC to prove ownership and gain super admin access
- An authoritative person should create a new XIQ account for the organization
- Devices must be connected/online in Classic to push updates to devices

Global Technical Assistance Center (GTAC) for Immediate Support
Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826.
For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Important considerations you must address prior to initiating a migration:

- HM Classic **configuration elements are not preserved**. When you export your HM Classic VHM, the configuration parameters are preserved in the exported file, but the configuration elements (such as network policies) are not preserved. This means that you may create the configuration elements in XIQ before importing the backup file from HMC or HMNG. If you finish configuring XIQ after importing the backup file you'll simply re-assign Network Policy and Locations.
- Device compatibility is important to address in the planning process
- FYI... ExtremeCloud IQ backup **configuration elements are preserved**. When moving your virtual IQ instance (VIQ) from one ExtremeCloud IQ account to another, the process is much easier since all the configuration elements are present in the export file and preserved during the transition.

Table of Contents

KEYS TO SUCCESS CHECKLIST	4
WEBLINKS	5
PLATFORM TERMINOLOGY.....	6
WHAT PLATFORM ARE YOU CURRENTLY USING?.....	6
DEVICE COMPATIBILITY.....	7
SETUP CLASSIC HM ACCESS	8
STEPS TO FIX A CLASSIC BACKUP THAT IS FAILING TO IMPORT DUE TO DATABASE SIZE	8
DOCUMENTATION	9
DEVICE IP DISCOVERY.....	11
LICENSING AND COST.....	12
EXPORT LICENSE KEYS – CLASSIC HM.....	14
THIRD-PARTY INTEGRATIONS.....	15
<i>ID Manager</i>	15
<i>Library SIP</i>	15
DOCUMENT DEVICES, SSIDS, DEVICE TAGS & VLAN MAPPING	16
EXPORT MAPS TO PDF	18
MANUALLY SCRUB DEVICE TABLE TO THE DEVICE INVENTORY FILE	19
REVIEW UNCONFIGURED AND UNMANAGED DEVICES.....	20
EXPORT RUNNING CONFIGURATIONS.....	21
UPGRADE HIVEMANAGER VERSION.....	22
EXPORT BACKUP CLASSIC DATABASE	23
DEVICE FIRMWARE VERSIONS	24
DEPLOYING EXTREMECLOUD IQ – PUBLIC CLOUD.....	25
ADDITIONAL ADMINISTRATORS.....	25
LICENSING	26
FIREWALL CONFIGURATION GUIDE.....	27
IMPORT BACKUP FROM CLASSIC.....	28
VERIFY IMPORT WAS SUCCESSFUL.....	29
USE APIS TO MOVE MAPS FROM LOCATIONS TO FLOORS.....	30
CONFIGURE EXTREMECLOUD IQ – NETWORK POLICY	31
DEPLOYING EXTREMECLOUD IQVA – ON-PREM.....	32
MIGRATING DEVICES TO XIQ PROCEDURE.....	33
MIGRATING ACCESS POINTS PREPARATION.....	34
MIGRATING SR SERIES NETWORK SWITCHES PREPARATION.....	34
<i>Update Certificate for SR2200 & SR2300 Series Switches</i>	36
MIGRATING A CLOUD VIRTUAL GATEWAY (CVG) & BRANCH ROUTERS (BR#) PREPARATION	38
CLASSIC INTERFACE MIGRATION STEPS.....	39
<i>Change CAPWAP Primary and Backup Server Target</i>	39
<i>Update Classic Devices to Make the Move to XIQ</i>	40
XIQ INTERFACE MIGRATION STEPS.....	42

CLIENT ROAMING BETWEEN HM CLASSIC AND XIQ APS	44
SCRIPTS	46
CREATE LOCATION, BUILDING, & FLOOR OBJECTS	46
FIX MAP & DEVICES ON LOCATION OBJECTS IN XIQ.....	48
REPORTS	54
ACCESS POINT COUNTRY CODES VERIFICATION.....	55
TROUBLESHOOTING.....	56
CALL TO ACTION	58

Keys to Success Checklist

Documentation > _____

Migrate or Address Licensing > _____

Backup Classic and Restore in XIQ > _____

XIQ Configuration > _____

Migrate Single Device > _____

Test > Test > Test > _____

Schedule Outage Window > _____

Complete Migration for a single site/building > _____

Repeat by migrating subsequent sites > _____

Review any support cases submitted by your users and adjust the configuration as necessary > _____

Success!

Highly recommended to do the following tasks:

- Backup Classic and spin up a local virtual instance and restore it. This is an invaluable tool at your disposal. You confirm you have a solid backup which you've verified by restoring it. Trust me when I say you'll find this useful during the migration. If you're working with Classic Public Cloud then gain access to that at a minimum.
- Export Maps to PDF and ensure the hostnames are visible especially if you don't have a local copy of the virtual machine.
- Device inventory export to .csv file
- Export the running-config from at least one AP & one Branch Router per network policy
- Export the running-config from every SR Switch and CVG/VGVA (IPsec tunnel aggregation endpoint)
- After you create a new customer XIQ instance, give yourself External Admin access (Extreme/Partner Administrator)

Weblinks

Here's a list of web links that are great resources to get started with XIQ:

- Great starting place for a person to begin their Extreme journey from Aerohive:
<https://www.extremenetworks.com/aerohive-useful-links/>
- Primary site for Cloud system information: (CLI, Guides, MIBs, Help File, etc.)
<http://docs.aerohive.com/>
- XIQ Virtual Appliance Info:
<http://docs.aerohive.com/330000/docs/help/english/ng/Content/reference/virtual-appliance-release-notes.htm>
- XIQ Virtual Appliance QuickStart Guide and Server Hardware Requirements:
<http://docs.aerohive.com/330000/docs/help/english/ng/Content/reference/guides/qsg-virtual-appliance.htm>
- Aerohive End of Life: <https://www.extremenetworks.com/support/end-of-sale-and-end-of-support-products/> > Aerohive EOS menu
 - > **Access Points** tab: check when access points go end of life
 - > **Routers & Switches** tab: check when routers and switches go end of life
 - > **Management** tab: check when the platform will go end of life
 - > **Support** tab: check when older support terms go end of life

Platform Terminology

HiveManager Classic = HMOL or HM Classic or Classic, VA = Virtual Appliance (VMWare)

HiveManager NG = HMNG or NG, VA = Virtual Appliance (VMWare)

ExtremeCloud IQ = XIQ

- XIQ Connect – No cost consumer-grade cloud management for basic “set it and forget it” deployments
- XIQ Pilot – Subscription-based Enterprise Cloud Management
- XIQ Co-Pilot – Tiered Cloud Management License; ML/AI to assist the admin with identifying issues and making recommended remediations (public beta)
- XIQ Auto-Pilot – Tiered Cloud Management License; Actionable AI (roadmap)
- IQVA – ExtremeCloud IQ On-Prem Virtual Appliance (VMWare)

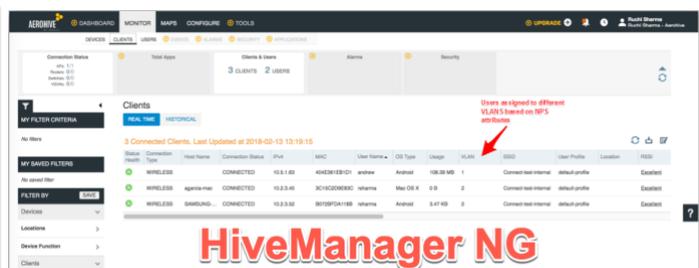
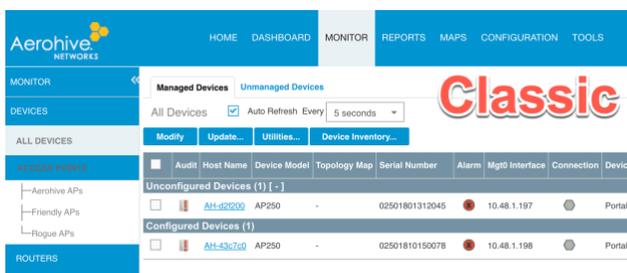
XIQ can be hosted...

- Public – AWS, Google Cloud - GCP, Microsoft AZURE (reach out to GTAC if a target platform is desired otherwise the XIQ account registration will pick one for you)
- Local VA – Single host in VMware
- Private – Our Cloud Architecture deployed on your hardware, in your DC or cloud of choice; Large MSP/Customer with white-label options. This requires PLM involvement so engage your Account team if this is of any interest.
- Cloud Edge – a three-tiered server cluster hosted in your DC provided by Extreme Networks as a Hardware & Software as a Service subscription. Fully managed by Extreme’s DevOps teams.

What Platform Are You Currently Using?

Browse to your HiveManager and look at the URL:

- If it’s a local IP address or URL then it’s on-prem: hostname.YourDomain.com
- If it’s <https://myhive.aerohive.com/> or similar to this address <https://hm-useast-497.aerohive.com/>; it’s in the public cloud
- You would only see HiveManager NG on-prem. The cloud version was upgraded to XIQ.



Device Compatibility

Supported Hardware List: <https://docs.aerohive.com/330000/docs/help/english/ng/Content/learning-whats-new.htm>

Access Points, SR Switches, & Routers:

- FYI... 802.11ax APs, ATOMs, and XR Series Branch Routers are not compatible with Classic
- Looking at XIQ Device Templates for compatibility is an option to double-check but shouldn't be the source of truth: Network Policy > Device Templates tab > AP Templates tab > +
 - In the past, IQVA is plumbed for new models but it's not quite supported until full device GA then IQVA typically needs an upgrade for full compatibility
- BR100 and all other variants of BR200-?? are not supported. We no longer sell or support a router with a built-in cellular router.
- BR200WP is supported with one caveat. The wireless radio is disabled so the SD-WAN features can be enabled. You would need to add an AP to the site for Wi-Fi connectivity after migrating.
- Physical Cloud VPN Gateway (CVG) appliances are not supported in XIQ and should be replaced by the Virtual Gateway Virtual Appliance (VGVA) or the XR600 physical router
- Often overlooked, this Aerohive Switch model is not supported: SR2024 <- No 'P'
- SR2024 & SR2024P switches have the capabilities of being a VPN tunnel terminator, using USB cellular AirCards for Internet, hosting DHCP servers, & performing layer 3 functions. These features are not supported in the XIQ GUI but can be achieved with S-CLI. As mentioned above the SR2024 is not supported in XIQ but the SR2024P model is.

Setup Classic HM Access

Partner or Field SE:

HMOL: Have the customer provide you credentials, preferably a new account for remote access. You can't use an email address if it is assigned to an existing HMOL account. If you're an Extreme employee you can use: `<your-email>+<anything-here>@extremenetworks.com`. You will receive an email containing the password. Email `name+alias@gmail.com` works too.

On-Prem: Set up remote access to current HM and/or create a lab VA to work from:

- Creating a lab Classic VA – Setting up a lab VA is beyond the scope of this doc, below is an overview. This was on the highly recommended list. See [Weblinks](#) for XIQ VA Quick Start Guide as it's similar.

Process Overview

- Create a new VM using the same version HM (ova) as what the customer is running in their environment. Partners may reach out to GTAC or their Extreme field SE. An Extreme Field SE may reach out to GTAC or the Solutions Architect team.
- Boot the VM and set up network settings using the console
- Open web UI via the assigned static IP address
- **IMPORTANT:** Create a new user on the existing Classic instance with Super User privileges so you don't have to exchange passwords. Once you restore you'll need credentials to get in.
- Take Classic backup of the VHM
- Import the configuration only backup provided by the customer's Classic instance (see [Export Backup Classic Database](#) section)

Customer:

- Verify you have a backup of your VM, a snapshot, and store your backup file from Classic in a safe place. Protect and plan so Murphy's Law does not apply. It just feels good that you have it.

Steps to fix a Classic backup that is failing to import due to database size using a Mac OSX:

- Customer has on-prem Classic. You spin up the same version VM in your lab. Many times the backup file is so large that you have issues with restoring the backup.
- Steps:
 - Extract the compressed backup file to a folder (Right Click > Open With > Archive Utility.app works well)
 - Navigate to `/HiveManager/downloads/home/image/<delete everything in this folder>`
 - Firmware is the culprit here, so those must go
 - Open a terminal window to the root folder level
 - Command: `tar -cvzf <Name>.tar.gz *`
 - The new file is one folder lower

- Use that file when importing into Classic using the same version:
 - You can upgrade the version of Classic from this point if necessary to get the Backup to HMNG feature.
- If anyone figures out how to accomplish the same thing in Windows please forward to the author Mike Rieben (mrieben@extremenetworks.com)

Documentation

- Document everything you can! Once a device is removed from Classic Public Cloud, the configuration & map location are gone. However, if you restored a backup to a lab VM you're ready for just about anything. You do not need to delete devices with on-prem deployments. Ultimately the VM will be shut down along with the devices.
- Maps with walls and devices are migrated through the backup and restore process, so verify locations & maps migrated completely before you remove a single device from Classic
- Anyone that is attempting to marry two or more sets of map data into a single XIQ instance. The names of each location & building must be unique. Floors may have duplicate names. The floor plan file names must also be unique. Each image is uploaded with the original file name.

Here are some gotchas to make note of:

- Are access points using one or two Ethernet cables? Are they set up as redundant or aggregate configurations?
 - You can see this in the monitor device table under LLDP Eth0 & Eth1 columns or
 - You may also look at each device level configuration for Eth0 & Eth1 configuration
- Are any access points acting as a DHCP server?
 - Look under Menu: Configuration > Advanced Config. > Common Objects > DHCP Server...
 - If any entries exist then you need to hunt for the AP using it at the device level
- Are Device Tags used? If so, make sure you document SSID and VLAN mappings. The export of devices includes tags per device. Shows up blank if they're not utilized.
- Are there SSID overrides disabling them on individual radios? The only way to figure this out is to look at the SSID's at the device level configuration. If you determine there are individual overrides you must document each one individually. This takes a lot of time. Discuss if this is imperative to accomplish business goals.
- Extreme AP's acting as a RADIUS server with a local directory. You will see this in the SSID config.

- Extreme AP's acting as a RADIUS proxy. Menu: Configuration > Advanced Configuration > Authentication > RADIUS Proxy
- Layer 2 policy-based routing by splitting traffic per Ethernet interface can be accomplished by Supplemental-CLI. The configuration in Classic is at the device level. Ask the question to the customer to determine if this is in place or go hunting. You can review all S-CLI objects within the Common Objects menu.

Final food for thought:

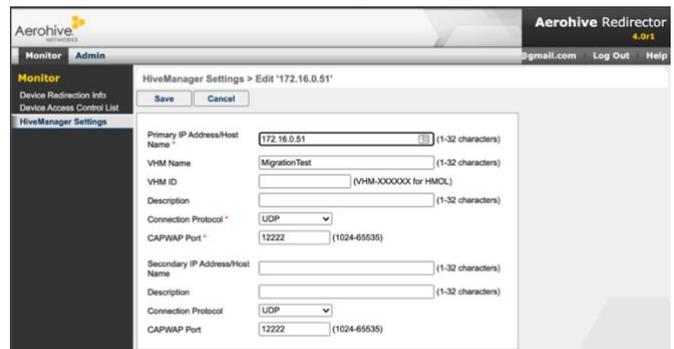
- It's up to you to determine the level of detailed documentation. It's a way for you to get familiarized with the environment. Often you and the customer are reverse-engineering the configuration together. You will capture it for posterity regardless and you'll use it for reference. You'll want to bring up the Classic interface side by side as you configure XIQ.
- When in doubt the running configuration is what is running live so use this as a source of truth

Menu: Configuration > All Devices > Checkmark device > press Utilities > Diagnostics > Show Running Config

Device IP Discovery

You may or may not know that a device connected to a Classic HMOL VHM get their Primary CAPWAP Server IP address from the redirector. Since XIQ uses the same process, a migration from Classic HMOL to XIQ is familiar. When migrating from a Classic On-prem to XIQ, the Primary CAPWAP Server IP address discovery is different. This process has to be accounted for so that devices don't migrate back to the Classic HM after migrating to XIQ.

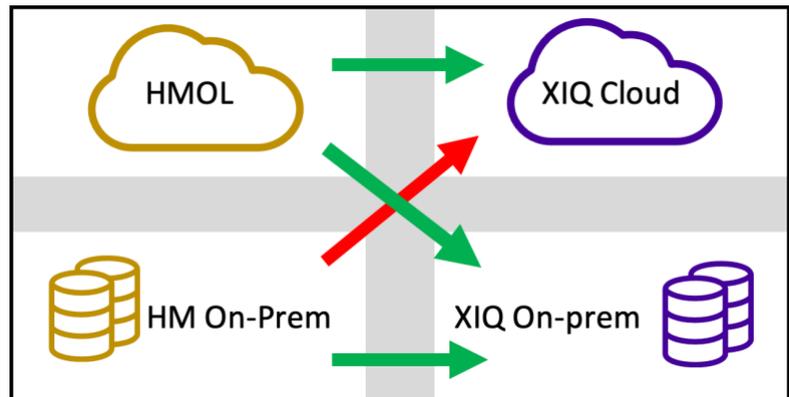
- On-prem HiveManager IP Discovery Options:
 - Static CLI Configuration of the CAPWAP Server:
 - i. `capwap client server name <IP Address>`
 - Dynamic CAPWAP IP discovery
 - i. DHCP Option **43**, Sub-Option **226** (Appliance IP), Sub-Option **225** FQDN
 - ii. DNS Query (hivemanager.yourdomain.com)
 - iii. L2 Broadcast
 - ^ can be disabled via AP CLI: `no capwap client discovery method broadcast`
 - iv. Disable these at the time of migration so that your migrated APs don't move back. Alternatively, you may deploy your new VA in a different L2 network.
 - v. This CLI will determine which IP the AP's reaching out to: `show capwap client`
- Cloud Redirector for On-prem HM:
 - This makes the process like an HMOL but the redirector simply tells the AP what the local IP address of HiveManager is. You add all device serial numbers to the cloud redirector which is tied to your MyHive cloud account. If the customer has it already set up, and all serial numbers are entered for Classic devices, you can simply update the IP address to the new IQVA local address. This is not available for new customers and will be deprecated upon the shutting down of our Classic systems. Highly recommended to migrate to one of the standard methods above.
 - To enable a device in XIQ you flip from unmanaged to a managed state. At that point, the serial number is validated to not exist anywhere else in the cloud. If the device is in the redirector then you will get an error. Open a GTAC case to investigate if this individual redirector system is in place. You may find that no one is left at your company that knows how to manage it. You access the redirector interface by going to myhive.aerohive.com.



Licensing and Cost

- Perpetual licensing is no longer offered. XIQ Pilot Term Based Licensing aka Subscription comes in yearly increments plus hardware maintenance per device.

- Migrating from **HMOL Public Cloud** to **XIQ Public Cloud**: **no cost**



- Simply copy and paste the legacy license keys over to XIQ and link to the support portal for any new licensing.

- Migrating from **HM Classic on-prem** or **HMNG on-prem** to **XIQ Pilot On-prem**: **no cost**

- If a customer has perpetual or legacy subscription entitlement keys then there's a step for anyone with Aerohive license server access to release the keys tied to the existing Classic instance. GTAC can assist if you're a partner or customer following this guide.
 - If you're moving permanent keys from **Classic On-prem** to **XIQ On-prem** try to move the keys by a simple copy and paste. Some keys may move over even though they're all technically in use. Extreme SA/SE: Connect to HiveManager Classic & NG license servers, filter to find the key(s), initialize in BOTH servers to free it up. Try adding them to XIQ and if you're denied, **Classic On-prem** pulled the key again since the VM was running.

Here's the workaround:

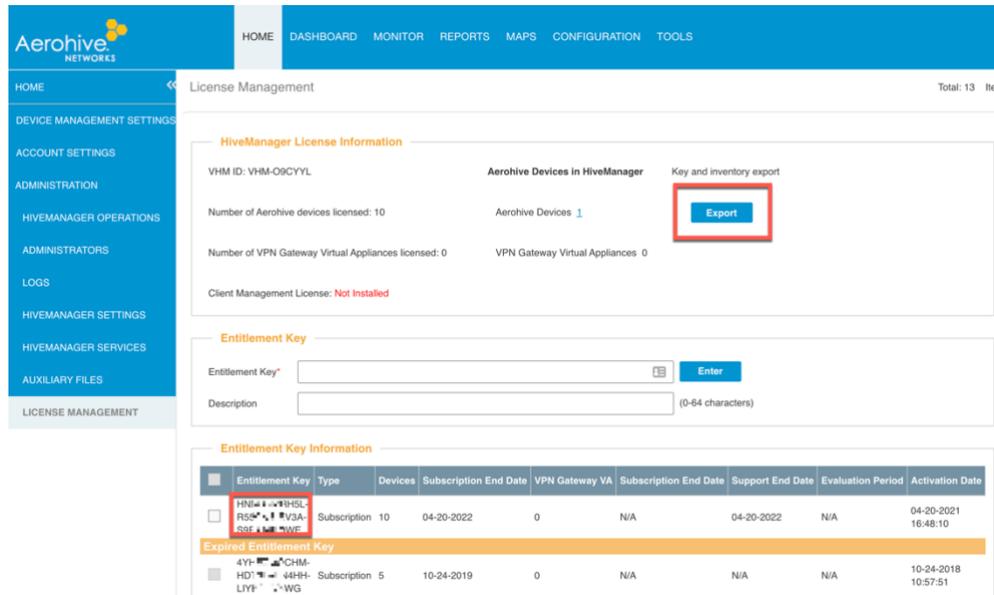
- Add a 90-day temp key to **Classic On-prem** just to make sure there are no license issues. You don't want the devices to change to an *Unconfigured* state. If they become in that state you will have to push a complete configuration push to fix them after licensing is addressed.
- Shut down the **Classic On-prem** VM, initialize the key in the BOTH license servers once more, add the key to **XIQ**, boot up **Classic On-prem** VM then verify all is well.
- Migrating from **HM Classic On-prem** or **HMNG On-prem** to **XIQ Public Cloud**: **conversion cost**
 - Contact your Extreme Account Team to work with the Renewals team to prepare a conversion plan

- ID Manager was a license that is no longer applicable to XIQ:
 - Private Pre-Shared Key (PPSK) features for the most part were ported over to XIQ
 - An Extreme field Systems Engineer (SE) or Solutions Architect (SA) may contact GTAC and request a license extension while the migration is in progress. All others please reach out to your Extreme account team or the SaaS team.
- XIQ and IQVA use a new license server called License Entitlement Manager (LEM). While your existing keys (Legacy) may move over. All new licenses require you to link your XIQ to our support portal to access licenses. The objective is to make implementing licenses simpler. When you make a license purchase, no further action is required regardless of using the cloud or on-prem software.
 - Note: IQVA is undergoing a license revamp at the time of this writing so an intermediate solution is required. Reach out to your account team or our SaaS team to acquire the proper legacy entitlement keys for all new Pilot licensing during this time.

Export License Keys – Classic HM

Menu: Home > Administration > License Management > Press Export button or manually copy your active entitlement keys

You can ignore the expired keys. The export has them if you want to keep them for posterity.



The screenshot shows the 'License Management' page in the Aerohive interface. The left sidebar contains navigation options like 'HOME', 'DEVICE MANAGEMENT SETTINGS', 'ACCOUNT SETTINGS', 'ADMINISTRATION', 'HIVEMANAGER OPERATIONS', 'ADMINISTRATORS', 'LOGS', 'HIVEMANAGER SETTINGS', 'HIVEMANAGER SERVICES', 'AUXILIARY FILES', and 'LICENSE MANAGEMENT'. The main content area is titled 'License Management' and includes a 'Total: 13 Iter' indicator.

HiveManager License Information

VHM ID: VHM-09CYL Aerohive Devices in HiveManager Key and inventory export

Number of Aerohive devices licensed: 10 Aerohive Devices 1 **Export**

Number of VPN Gateway Virtual Appliances licensed: 0 VPN Gateway Virtual Appliances 0

Client Management License: **Not Installed**

Entitlement Key

Entitlement Key* **Enter**

Description (0-64 characters)

Entitlement Key Information

Entitlement Key	Type	Devices	Subscription End Date	VPN Gateway VA	Subscription End Date	Support End Date	Evaluation Period	Activation Date
HRN...RSE...SSE...WG	Subscription	10	04-20-2022	0	N/A	04-20-2022	N/A	04-20-2021 16:48:10
Expired Entitlement Key								
4Y...HD...LTY...	Subscription	5	10-24-2019	0	N/A	N/A	N/A	10-24-2018 10:57:51

Third-Party Integrations

Review the HiveManager Services page by navigating to Menu: Home > HiveManager Services

✗ : 3rd party or feature is not supported in XIQ

✓ : This service is available in XIQ

ID Manager

As mentioned earlier, ID Manager is no longer an add-on license. The majority of features have been rolled into XIQ natively under Private Pre-Shared Key (PPSK).

- An Extreme field Systems Engineer (SE) may contact GTAC and request a license extension while the migration is in progress

Library SIP

There's one more third-party integration located in the Authentication section called *Library SIP*. Aerohive devices can function within a SIP2 (Standard Interchange Protocol, version 2) environment to provide self-service access to library resources. This feature is not supported in the XIQ GUI.

Classic Menu: Configuration > Show Nav > Advanced Configuration > Authentication > Library SIP Access Policies

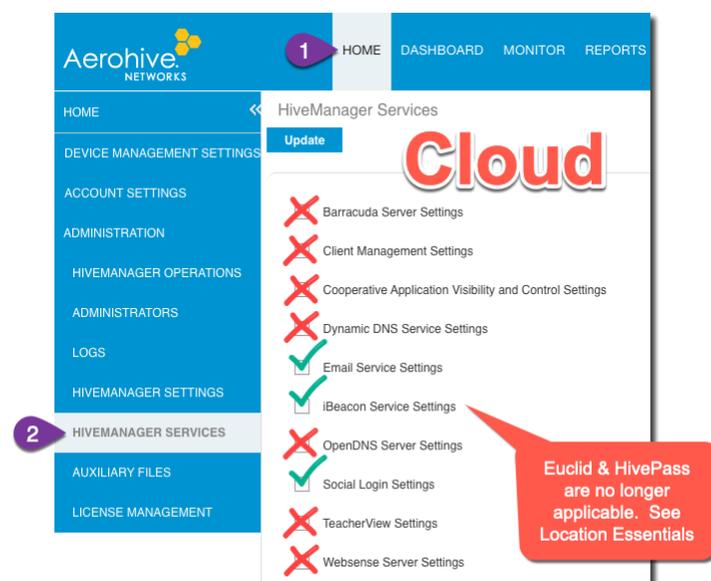
You can port over the CLI configuration to XIQ using S-CLI since the IQEngine OS, formerly HiveOS, supports these commands. You will need to pull the running configuration and manually migrate it to XIQ.



On-Prem

- ✗ AirTight SpectraGuard Enterprise (SGE) Integration Settings
- ✓ Application Visibility and Control Settings
- ✗ Barracuda Server Settings
- ✓ CAPWAP Server Settings
- ✗ Client Management Settings
- ✗ Cooperative Application Visibility and Control Settings
- ✗ Customer ID Retrieval
- ✗ Dynamic DNS Service Settings
- ✓ Email Service Settings
- ✓ HiveManager Admin Authentication Settings (Local)
- ✗ HiveManager TFTP Service Settings (Off)
- ✓ iBeacon Service Settings
- ✓ Log Server Settings
- ✓ Notification Information Settings
- ✗ OpenDNS Server Settings
- ✓ Presence Analytics Settings
- ✗ SNMP Server Settings
- ✗ Social Login Settings
- ✗ StudentManager Settings for Remote Access Credentials
- ✗ TeacherView Settings
- ✗ Websense Server Settings

Euclid & HivePass are no longer applicable. See Location Essentials



Cloud

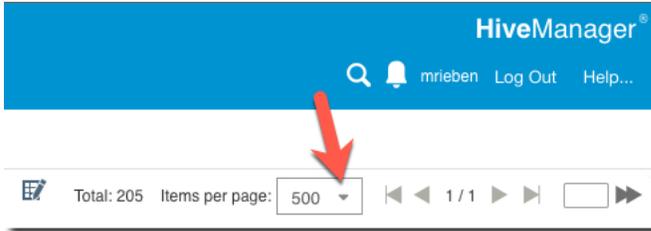
- ✗ Barracuda Server Settings
- ✗ Client Management Settings
- ✗ Cooperative Application Visibility and Control Settings
- ✗ Dynamic DNS Service Settings
- ✓ Email Service Settings
- ✓ iBeacon Service Settings
- ✗ OpenDNS Server Settings
- ✓ Social Login Settings
- ✗ TeacherView Settings
- ✗ Websense Server Settings

Euclid & HivePass are no longer applicable. See Location Essentials

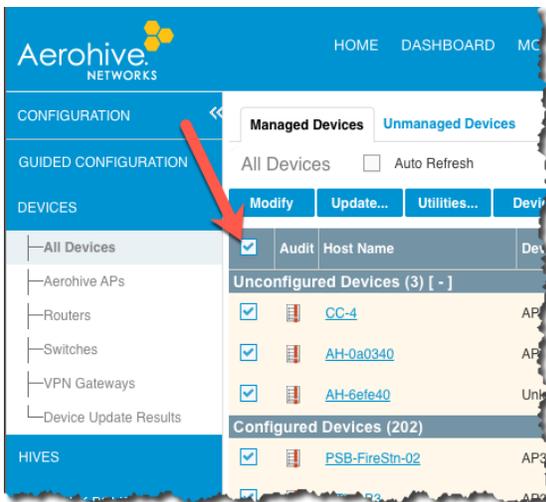
Document Devices, SSIDs, Device Tags & VLAN Mapping

Navigate to Menu: Configuration > Devices > All Devices

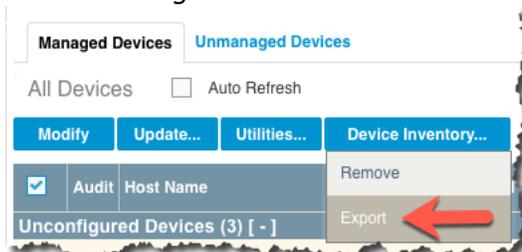
- Adjust the row display to 500



- Checkmark to select all devices



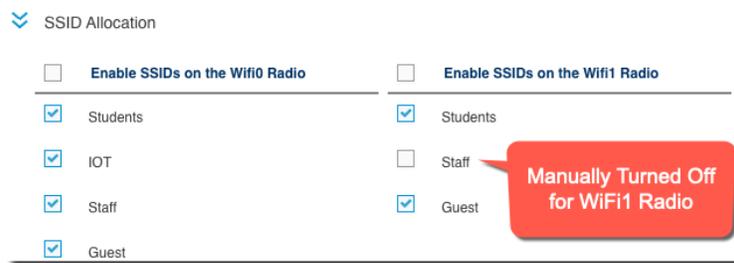
- Press Device Inventory... button > Export (Repeat for each set of 500 pages)
 - If you do not have the Export or Remove menu then you're not an administrator
 - The *Unmanaged Devices* tab contains any devices that were added but never checked in



- Save your CSV file then open in Excel or any spreadsheet program
- Review Device Tags: (if columns are blank then these aren't used)
 - RED**: Sometimes the HiveOS versions needs to be moved over one row since they appear under TAG1
 - GREEN**: These are Device Tags

X	Y	Z	AA
HiveOS	TAG1	TAG2	TAG3
8.1r1			
10.r.			
8.2r4			
	6.6r1	GH_Prod	
6.6r2			
	6.5r5		
	6.5r5		
6.5r6		187	
6.5r6		191	

- Devices tags can be used to assign VLANs based on the tag assignment at the device level and within the User Profile, so these are critical to map VLANs properly when configuring XIQ
- There are multiple device level overrides to be aware of.
- Navigate to Menu: Configuration > Aerohive APs > (click hostname) > (expand SSID Allocation)



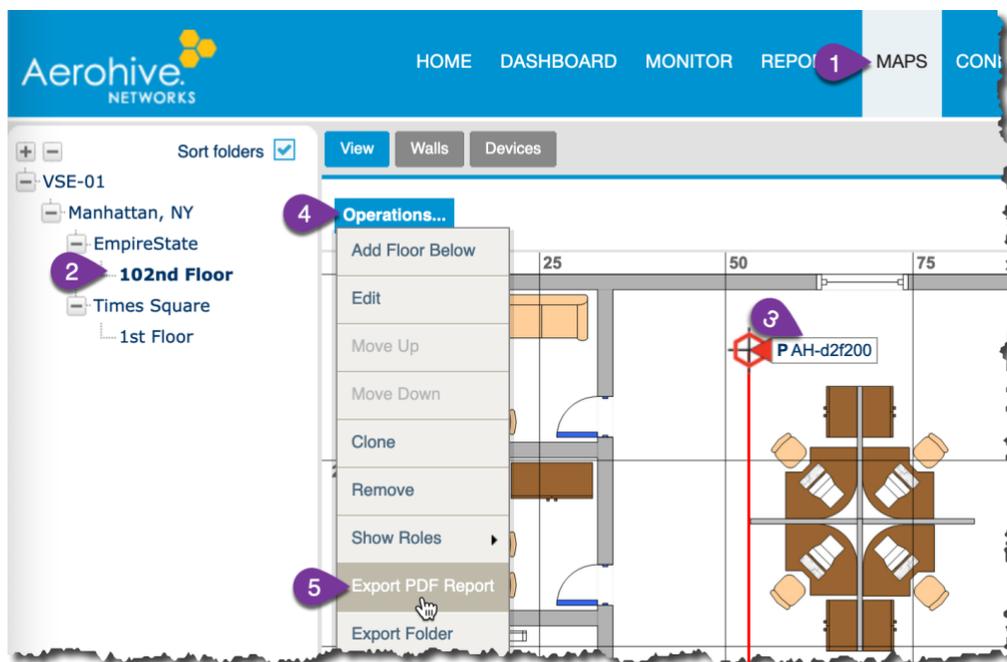
All SSIDs are viewable here: Menu: Configuration > SSIDS

- The question you can't answer is if all user-created SSIDs are being actively being used
- If you find manual overrides you need to check every AP and document which AP and Wi-Fi radio is using which SSID

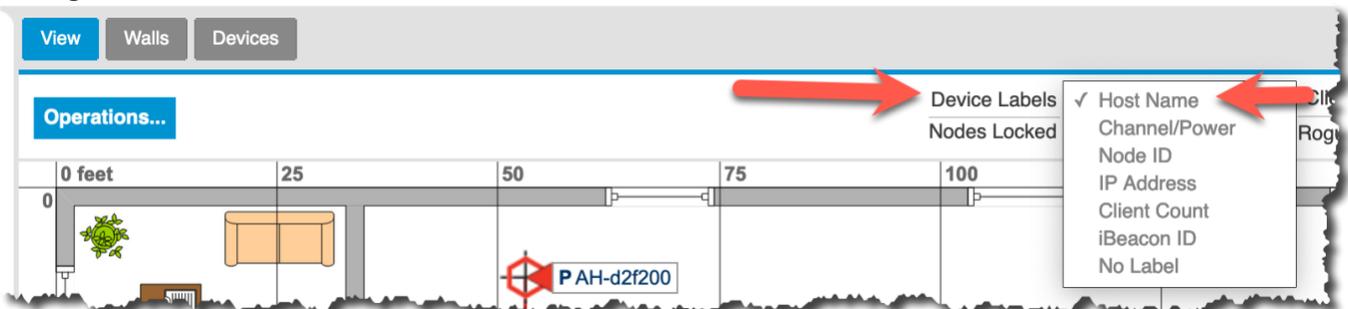
Export Maps to PDF

This step is optional and may be skipped if you will confirm you have a solid backup and restore to XIQ before deleting any devices. I personally like to preserve information via PDF for posterity but up to you and your time constraints.

1. Navigate to Menu: Maps
2. Expand locations to where your floor plan is
3. Verify your devices are showing Hostnames
4. Press Operations... button
5. Choose Export PDF Report

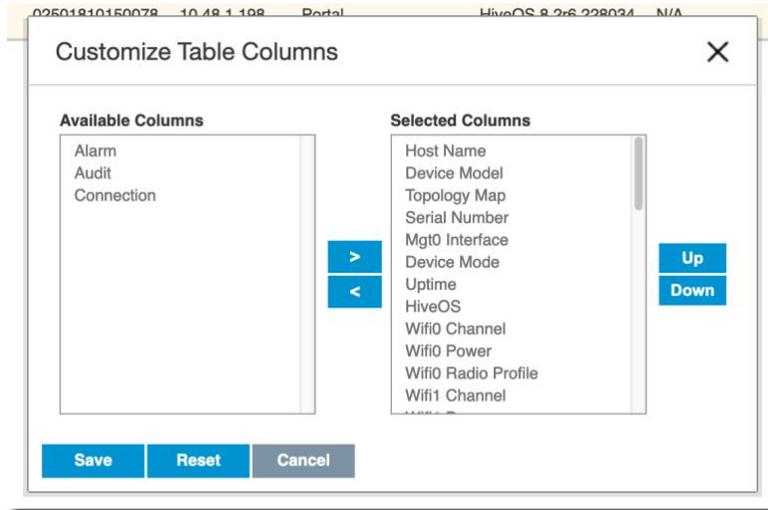


Change Device Labels:



Manually Scrub Device Table to the Device Inventory File

The export devices capture a lot of information however the Monitor table has a lot more to offer. Click the column picker and add everything available. Then remove the columns that contain icons since Excel doesn't deal with those very well. (Alarm, Audit, Connection)



Click and drag to select the entire table:



	Host Name	Device Model	Topology Map	Serial Number	Network Policy	Node ID	SDR Profile	Supplen
<input checked="" type="checkbox"/>	AH-d2f200	AP250	Empirestate_1st Floor	025018	255.0 VSE-01	C413E2D2F200		
<input checked="" type="checkbox"/>	AH-43c7c0	AP250	Times Square_1st Floor	025018	255.0 VSE-02	F4EAB543C7C0		

- Copy clip the highlighted text then open your Device Inventory CSV spreadsheet
- Save it as an XLSX file so you can edit without any formatting issues
- Create a new tab
- Paste the copied table information
- Repeat for every 500 devices

You now have a lot more information captured for future reference. Don't forget to return the columns how you found them.

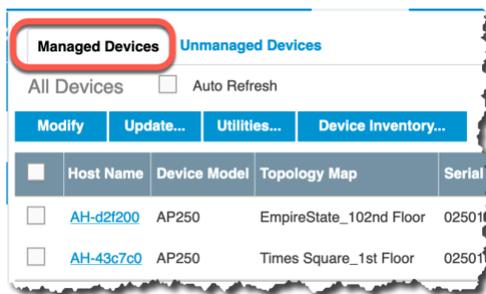
Review Unconfigured and Unmanaged Devices

Navigate to Menu: Monitor

The **Unconfigured Devices** tab are devices discovered by HiveManager Classic and formed a CAPWAP connection but have not yet received a configuration.

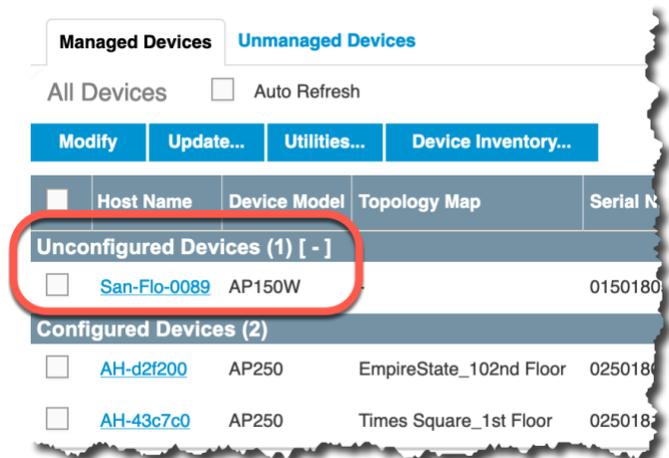
The **Unmanaged Devices** tab lists devices that have not yet established a connection with HiveManager Classic. They were added via serial number but haven't established CAPWAP with Classic.

Warning: Devices listed in the Unmanaged Devices tab do not migrate with the export and import process. Those will have to be removed from Classic using *Remove* under the Device Inventory button then add them manually in XIQ.



If all your devices are in an “Unconfigured” state then one possibility is the Classic instance had expired licenses. Once license issues are resolved the devices need a complete configuration push to return them to a configured device state.

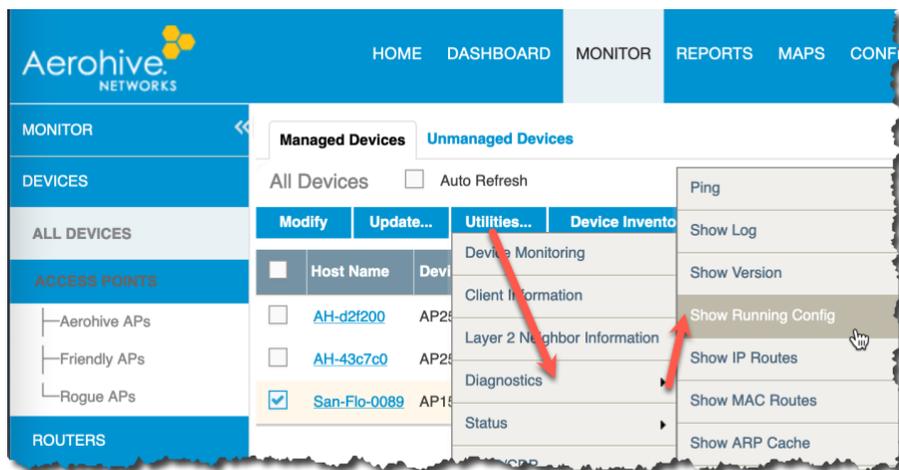
In this case, the device is not assigned a Network Policy and never received a configuration but has checked into Classic via a CAPWAP connection. →



Export Running Configurations

Navigate to Menu: Monitor

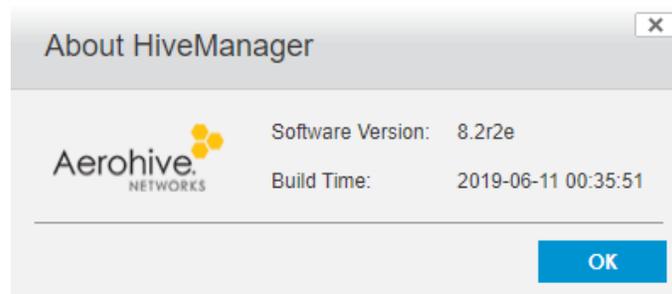
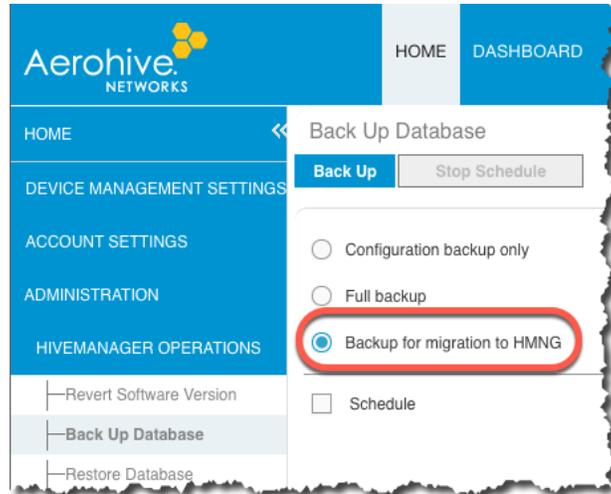
- Checkmark a single device > Press Utilities > Diagnostics > Show Running Config
- Highlight and copy the output
- I recommend using the same Device Inventory spreadsheet. Create a new tab for CLI configurations. Paste the copied info.



- This step is imperative for every switch since that is the best way to see what is currently running on the device. Some admins use CLI to configure switches even though they're cloud-managed.
- I've personally seen where the configuration in Classic was never pushed to the switch and therefore would've led me to configure XIQ incorrectly.

Upgrade HiveManager Version

Classic on-prem needs to be at 8.2r2e to be able to create a configuration backup for XIQ import.



If your HMOL (Cloud) has a buzzing bee in the top right corner you must upgrade to or newer the 8.2r2e version.

Export Backup Classic Database

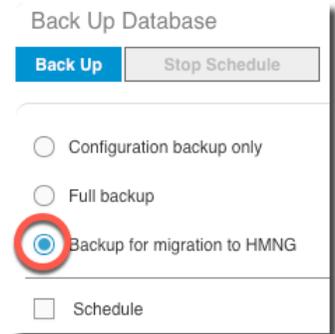
Prepare a backup file of HiveManager:

Menu: Home > Administration > HiveManager Operations > Back Up Database

If you don't see this option, you must upgrade to the latest Classic version. Yes, even if you're in the public cloud. Look for the buzzing bee.

If you plan to use this backup as your local offline access you must have credentials. Once you restore, the only access is by using one of the credentials already defined.

Note: If a scheduled backup is configured it will have to be deselected before either of the previously mentioned backups can be run. Be sure to document the scheduled backup configurations before deselecting them. Once deselected, the scheduled backup configurations are lost.



Device Firmware Versions

If it's not necessary to upgrade your firmware, skip it while devices are connected to Classic. Once the AP connects to XIQ it will get the latest firmware available which is defined in XIQ device templates.

Firmware version HiveOS 6.5.11 and some older 6.5.X will migrate fine. If you encounter any issues with the AP checking into XIQ you can either manually upgrade the firmware using the device's web interface or add them back to Classic and upgrade from there.

I recommend you review this section: [Device IP Discovery](#)

- When a device isn't checking in, the issue may lie with which instance the device is trying to communicate to. Classic or XIQ... that is the question.

If you're having any issues with pushing configurations while in Classic, refer to the firewall configuration guide for HiveManager Classic Public Cloud:

https://docs.aerohive.com/330000/docs/help/english/6.6r1/hm/full/help.htm#ref/services.htm%3FTocPath%3DReference%2520Material%7CConcepts%2520and%2520Software%2520Reference%7C_____8

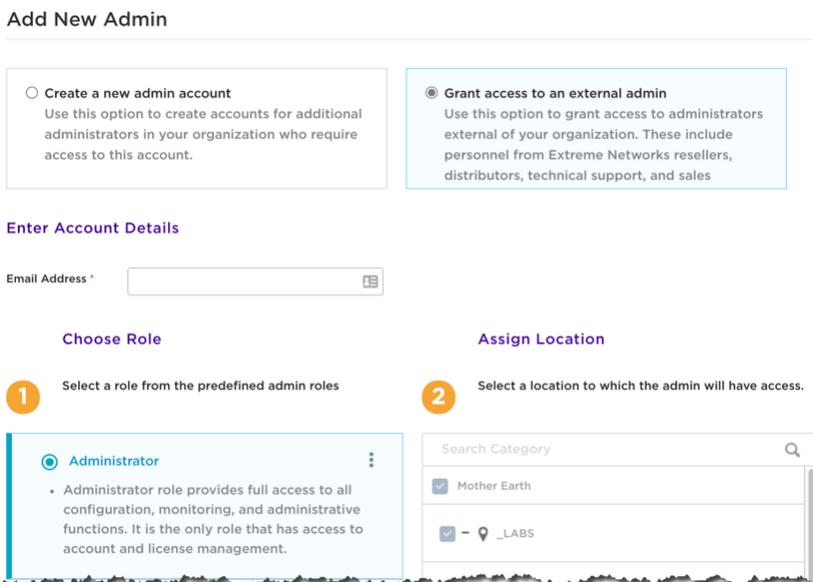
Deploying ExtremeCloud IQ – Public Cloud

- Register for an account: <https://extremecloudiq.com/login>
 - Only one person in the organization needs to register
 - Use the 30-day trial for the initial account creation. You can address licensing later since you more than likely have a combination of legacy entitlement keys and a support portal where new licensing is stored.

Additional Administrators

- XIQ: Have the customer add the person working the migration as an external admin to their XIQ account. This can be done by hovering over your name in the upper right-hand corner of XIQ, selecting Global Settings > Account Management > + Add User > be sure to select *Grant access to an external admin*:

Add New Admin



Create a new admin account
Use this option to create accounts for additional administrators in your organization who require access to this account.

Grant access to an external admin
Use this option to grant access to administrators external of your organization. These include personnel from Extreme Networks resellers, distributors, technical support, and sales

Enter Account Details

Email Address *

Choose Role

1 Select a role from the predefined admin roles

Administrator
Administrator role provides full access to all configuration, monitoring, and administrative functions. It is the only role that has access to account and license management.

Assign Location

2 Select a location to which the admin will have access.

Search Category

Mother Earth

- _LABS

- Choose Role: **Administrator**
- IQVA: External access option is not available through the software

Licensing

Navigate to Menu: Administration > License Management > click *Enter it here* for legacy keys

Legacy Entitlements

Do you have a Legacy Entitlement Key? [Enter it here](#)

- Enter each key you exported from Classic. You may ignore expired keys.
- Entitlement keys will be active in both instances during the migration until expiration
- The keys will eventually expire in Classic so just let it go 🎵

You must log out and back in to activate keys. If you purchased a new XIQ license in 2021 you should've received a Welcome to Extreme Networks email. If you do not have entitlement keys then they're in the support portal since that is the new delivery method.

- If you already have a support portal account you may click Extreme Licensing Portal and use those credentials to link XIQ. If not, go ahead and register for one as soon as possible. It takes a few days to tie in all the backend information. This is a one-time effort.
- Sample Welcome Email: (CUID is required to link your account, enter when prompted.)
- Also can be found in Extreme Network Salesforce (employees only)

License Information

[EXTREME LICENSING PORTAL](#)

Subject: Extreme Networks Support Contract Notification - Contract: 140000045, PO#: 200000000
 Body:
 Welcome to Extreme Networks!

We are thrilled to welcome you to the Extreme™ family. Our desire is to make your journey simple and enjoyable.

Agreement Account: 140000045
 Agreement Enduser Account: 140000045
 Distributor PO Number: 200000000

Reseller PO Number: 500000000

Contract Number
 140000045

Contract Start Date (mm/dd/yyyy)
 02/11/2021

Contract End Date (mm/dd/yyyy)
 12/20/2022

CUID
 140000045

Customer User ID (CUID)

For Detailed Product Activation Instructions:

If you have an account on the Extreme Support Portal, please click on the product name noted below and select the 'Activation Instructions' navigation. If you do not have an account, see our Account Registration Instructions below.

Products:

ExtremeCloud IQ

ExtremeCloud IQ Pilot customers will no longer receive entitlement keys. For details on how to retrieve entitlements, please refer to licensing instructions in the link above.

Account Registration Instructions for Extreme Support Portal:

1. Go to <https://extremeportal.force.com>.
2. Select the Log In or Sign Up link on the top right.
3. On the Log In page, select the Create an Account link and follow the instructions. You will receive an email to complete the account registration process. It may take up to an hour to receive your email.
4. Please select a product from the Products listed above for activation and product related instructions.

Contract Details and CUID (Customer Unique Identifier) Reference Information:

Your Service Contract with Extreme Networks is attached. Please make sure to review your contract regarding the details of the attached service contract, please contact us within 10 days of receiving your contract can also be found on the Service Contracts Page of our Extreme Support Portal. Your CUID, noted above, is used during the installation and provisioning of some Extreme products. Please refer to the Detailed Product Activation Instructions at the top of this email.

For service renewal or service upgrade please contact:

Note: IQVA is undergoing a license revamp at the time of this writing so an intermediate solution is required. Reach out to your account team or our SaaS team to acquire the proper legacy entitlement keys for all new Pilot licensing during this time.

Customer Unique ID		SalesForce (Extreme)			Customer Unique ID Help
Action	CUID Name	Is Primary	Is Revoked	Shared	
	CUID-3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	rU-3t6	

Firewall Configuration Guide

CRITICAL STEP: Confirm your firewall adheres to the outbound rules as shown. Hover over your name in the top right corner in XIQ > About ExtremeCloud IQ > click Firewall Configuration Guide hyperlink.

This varies per Regional Data Center: (example shown is for RDC: VA2)

- Public IPs occasionally expand in scope as the cloud grows so keep an eye out for the communications menu to inform you of changes

FIREWALL CONFIGURATION GUIDES

Connectivity between Extreme cloud and the managed network is required. Ensure all in-line firewalls allow outbound connections to the following Extreme cloud services:

Global Data Center Services

Domain Name	IPv4 Addresses	Protocol	Port
redirector.aerohive.com	54.172.0.252	HTTPS	TCP 443
		HTTP	TCP 80
		UDP	UDP 12222
hmupdates-ng.aerohive.com	54.86.95.132	HTTPS	TCP 443
extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	TCP 443
	18.194.95.0 ~ 18.194.95.15		
	3.234.248.0 ~ 3.234.248.31		
	44.234.22.92 ~ 44.234.22.95		
cloud-rd.aerohive.com	34.253.190.192 ~ 34.253.190.255	HTTPS	TCP 443
stun.extremecloudiq.com	3.234.248.28, 3.234.248.29	UDP	UDP 12222
	18.194.95.14, 18.194.95.15		

UDP 12222
(CAPWAP)

US_East2 Regional Data Center Services

IPv4 Addresses Block	Protocol	Ports
34.202.197.0 ~ 34.202.197.63 3.234.248.0 ~ 3.234.248.31 44.192.245.0 ~ 44.192.245.63	HTTP	TCP 80
	HTTPS	TCP 443
	TCP	TCP 2083, 20000 ~ 20256
	UDP	UDP 12222

TCP 2000 ~ 20256
(SSH Proxy)

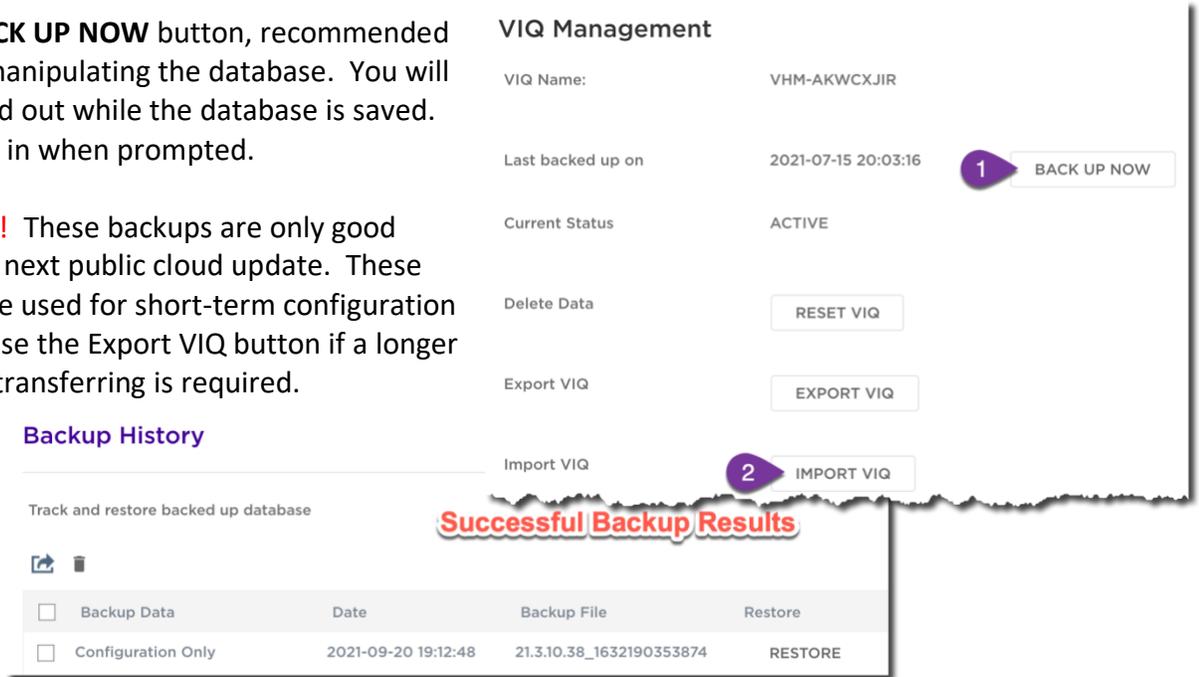
TCP 2083 (RadSec
Proxy – PPSK)

Import Backup from Classic

Locate the tar.gz backup file you exported from Classic. Hover over your name in the top right corner in XIQ > Global Settings > Administration > VIQ Management

1. Click **BACK UP NOW** button, recommended before manipulating the database. You will be logged out while the database is saved. Log back in when prompted.

Warning! These backups are only good until the next public cloud update. These should be used for short-term configuration saves. Use the Export VIQ button if a longer term or transferring is required.



VIQ Management

VIQ Name: VHM-AKWCXJIR

Last backed up on: 2021-07-15 20:03:16

Current Status: ACTIVE

Delete Data: RESET VIQ

Export VIQ: EXPORT VIQ

Import VIQ: IMPORT VIQ

Backup History

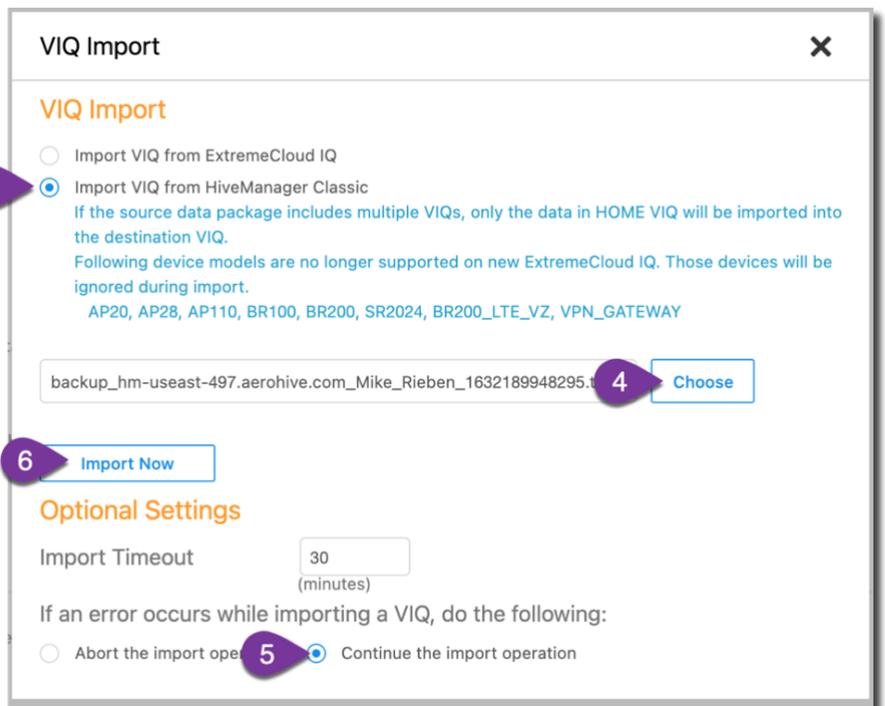
Track and restore backed up database

<input type="checkbox"/>	Backup Data	Date	Backup File	Restore
<input type="checkbox"/>	Configuration Only	2021-09-20 19:12:48	21.3.10.38_1632190353874	RESTORE

Successful Backup Results

2. Press **IMPORT VIQ** button
3. Choose *Import VIQ from HiveManager Classic*
4. Press **Choose** button then pick your Classic backup file
5. Choose *Continue the import operation*
6. Press **Import Now** button

There's one remediation step herein if an error occurs: [Click here for Steps to fix a Classic backup that is failing to import due to database size](#)



VIQ Import

VIQ Import

Import VIQ from ExtremeCloud IQ

Import VIQ from HiveManager Classic

If the source data package includes multiple VIQs, only the data in HOME VIQ will be imported into the destination VIQ.

Following device models are no longer supported on new ExtremeCloud IQ. Those devices will be ignored during import.

AP20, AP28, AP110, BR100, BR200, SR2024, BR200_LTE_VZ, VPN_GATEWAY

backup_hm-useast-497.aerohive.com_Mike_Rieben_1632189948295.tar.gz

Import Now

Optional Settings

Import Timeout: 30 (minutes)

If an error occurs while importing a VIQ, do the following:

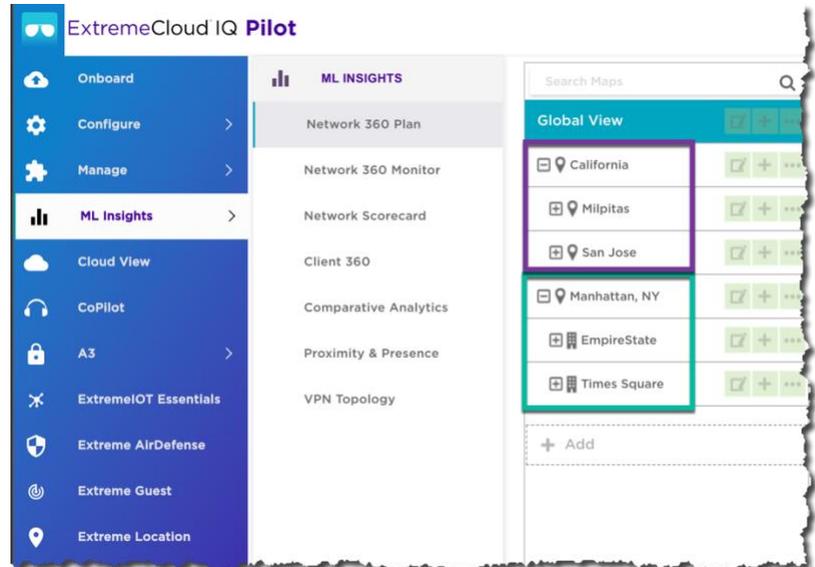
Abort the import operation

Continue the import operation

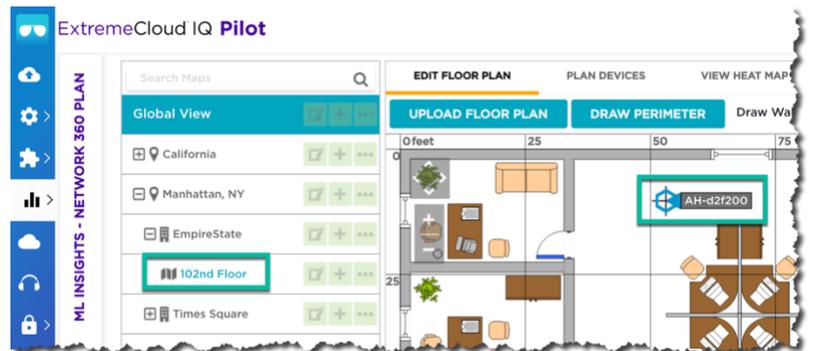
Verify Import Was Successful

Once the import is complete: verify your locations, maps, and devices imported. Navigate to Menu: ML Insights > Network 360 Plan

- These locations were present before the import was processed. The import was successful because none of the names in the Classic backup conflicted.
- These were the locations imported from Classic

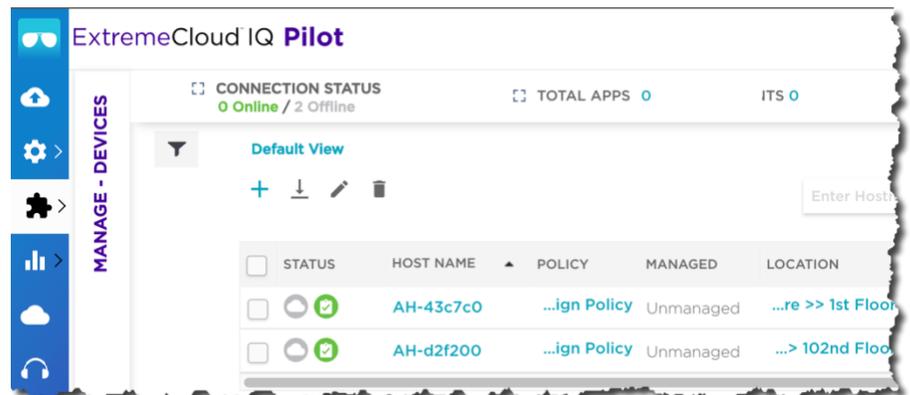


Expand a location and verify your map and devices are shown on the floor



Navigate to Menu: Manage > Devices

- Add the *Managed* column using the column picker  and notice that all devices are added as Unmanaged. That means that they can't communicate to XIQ and do not consume a license.
- Notice that the devices kept their hostname, location, & static IP's
- Network Policy wasn't imported, so it's Unassigned



Use APIs to Move Maps from Locations to Floors

In Classic the user was allowed by the GUI to add maps to a Location object instead of forcing them to apply it to a floor object which XIQ does. We've provided some Python/API scripts to help facilitate the moving of maps and devices from the location object to a floor.

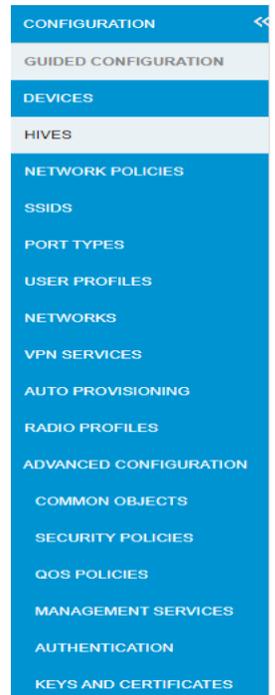
See section: [Fix Map & Devices on Location Objects in XIQ](#)

Configure ExtremeCloud IQ – Network Policy

Before you migrate your devices from Classic you should configure your Network Policy in XIQ but this is not a requirement. Configuring XIQ is outside the scope of the guide.

A method is to have two windows open and you compare, contrast, then create objects in XIQ.

a. **Build XIQ Configuration** - Manually recreate the Network Policy configuration from Classic to XIQ.



I. There are different ways of approaching this process.

- **Common Objects First** - Build all the common objects before creating the network policy. Start with the IP Objects and VLANs, then move to the bottom of the Management Services list and work from the bottom up the list.
 - i. Authentication objects, Local User Groups, CWPs, and RADIUS Servers can be created while building the Network Policies.
 - ii. Local Users can be imported any time after the Local User Groups are created.
 - iii. Looking at Common Objects is critical to not miss items but you also might be creating objects that aren't in use or will be abandoned as you choose what to move over. (DHCP, RADIUS Proxy, etc.)
- **Network Policies First** – This method starts with the network policies and creates the common objects as needed within the network policy. It is recommended that you minimize multiple network policies and use classification rules for multi-site deployments.

b. **Create Device Templates**

- XIQ uses device templates and minimal network policies that devices acquire their configuration upon onboarding. These features minimize the need for device-level overrides which makes managing network devices easier.

Deploying ExtremeCloud IQVA – On-Prem

Weblinks:

- XIQ Virtual Appliance Info:
<http://docs.aerohive.com/330000/docs/help/english/ng/Content/reference/virtual-appliance-release-notes.htm>
- XIQ Virtual Appliance QuickStart Guide and Server Hardware Requirements:
<http://docs.aerohive.com/330000/docs/help/english/ng/Content/reference/guides/qsg-virtual-appliance.htm>

Please draw your attention to this section:

This is the minimum recommended regardless of size:
 (Don't cut corners because the next release is going to consume more resources)

High-Capacity Virtual Machine Recommendations

The IQ Virtual Appliance OVA defaults to the high-capacity version.

Recommended minimum hardware requirements for deploying a total of 5000 APs or switches:

High-capacity Virtual Machine Recommendations (up to 5000 devices)
Xeon E5-2620 v4, 2.1GHz, 20MB cache or better CPU
8 CPU Cores, and 16 Threads
32 GB RAM
SSD (solid state drive)
300 GB of Storage Capacity

 IQ Virtual Appliance does not support storage area networks (SAN).

Notice the note about not supporting SANs. If you have a SAN that can achieve low ms latency and high IOps then you might be okay. If GTAC determines that the issues lie with the underlying hardware support will not continue until that issue is resolved. Not all SANs are created equal or misconfigured in many instances.

Migrating Devices to XIQ Procedure

On-Prem VA: Remove DNS 'A' record (hivemanager.yourdomain) and DHCP Option 43 prior or the access points will reboot and try to connect to a local instance instead of the cloud. If you're moving from VA to VA then update your 'A' record and DHCP options for the new IP address. [See discovery mechanisms here](#)

Make sure your devices are in a connected state in the Classic interface. Menu: Monitor > All Devices

- If they are disconnected you can't push a configuration update
- If the AP has a minimum firmware of HiveOS 6.5.X then you can simply locate and factory reset the AP. If you have any issues with onboarding the device you can manually upgrade the firmware using the web interface. Download the firmware from the support portal.

You should have the following complete at this stage:

- XIQ deployed
- Classic backup restored
- Location / Building / Floors established
- XIQ Network Policies configured
- All devices are assigned to a floor and a network policy
- Documentation is complete

You're ready to move a device from Classic to XIQ.

IQVA On-Prem - In a Classic On-prem deployment, you do not need to delete the device from the Classic HM when migrating. Most on-prem deployments do not use a redirector so there will be no conflict of having the serial number in the on-prem and XIQ. Eventually, this VA will be shut down.

On-prem with Cloud Redirector - In a Classic on-prem deployment, with the cloud hosted redirector, you will need to remove the device from the customer's redirector. Deleting the device out of the Classic VM will not remove it from their redirector.

It is highly recommended to migrate one device and test to validate your XIQ configuration. Repeat this process for each site that uses different configurations (SSIDs, VLANs, etc). Be methodical to ensure a smooth transition.

When in doubt reach out to GTAC +1-800-872-8440 and get some assistance to fill in the blanks. Climbing towers or ladders isn't ideal while in a hurry to fix an issue.

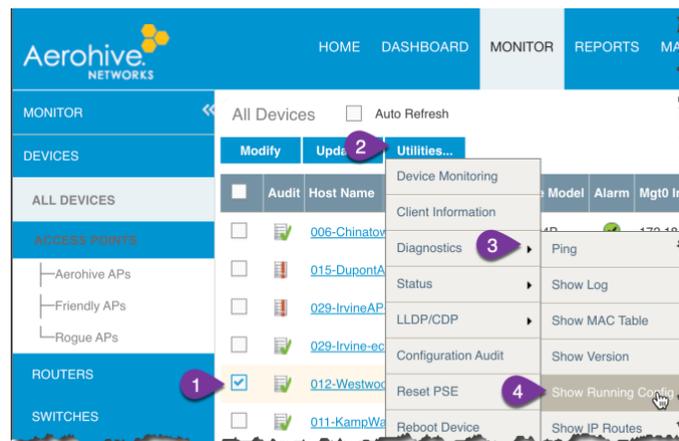


Migrating Access Points Preparation

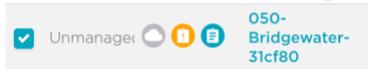
- At this point you've scrubbed the device information to a spreadsheet: [Document Devices](#)
- You should have your Network Policy configured:
 - SSIDs, Device Templates, Radio Profiles
- Exporting a running configuration is optional for access points

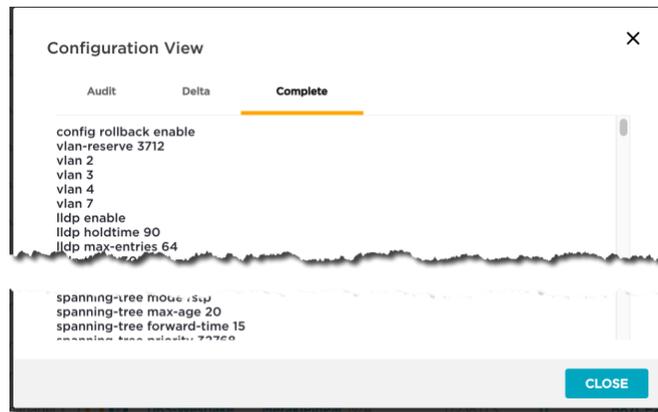
Migrating SR Series Network Switches Preparation

- At this point you've scrubbed the device information to a spreadsheet: [Document Devices](#)
- Export the running configuration of every single switch, one at a time, to your spreadsheet. Do not use the GUI to determine the final configuration. The running configuration is what is working today. This captures any method of configuring switches.



A	B	C	D	E
1	Switches - 84 Total		Example Switch Documentation	
2	1			2
3	Hostname:	000-LAB		001-Bethesda-ec2680
4		vlan 2		vlan-reserve 3712
5		vlan 3		vlan 2
6	LEGEND	vlan 4		vlan 3
7	Skip	interface eth1/1 switchport mode trunk		vlan 4
8	Problem	interface eth1/4 switchport mode trunk		vlan 7
9	Complete	interface eth1/3 switchport user-profile-attribute 2		interface eth1/1 switchport mode trunk
10		interface eth1/5 switchport user-profile-attribute 2		interface eth1/4 switchport mode trunk
11		interface eth1/7 switchport user-profile-attribute 2		interface eth1/3 switchport user-profile-attribute 2
12		interface eth1/9 switchport user-profile-attribute 2		interface eth1/5 switchport user-profile-attribute 2
13		interface eth1/11 switchport user-profile-attribute 2		interface eth1/7 switchport user-profile-attribute 2
14		interface eth1/13 switchport user-profile-attribute 4		interface eth1/9 switchport user-profile-attribute 2
15		interface eth1/3 switchport access vlan 2		interface eth1/11 switchport user-profile-attribute 2
16		interface eth1/5 switchport access vlan 2		interface eth1/13 switchport user-profile-attribute 2
17		interface eth1/7 switchport access vlan 2		interface eth1/15 switchport user-profile-attribute 4
18		interface eth1/9 switchport access vlan 2		interface eth1/3 switchport access vlan 2
19		interface eth1/11 switchport access vlan 2		interface eth1/5 switchport access vlan 2
20		interface eth1/13 switchport access vlan 4		interface eth1/7 switchport access vlan 2
21		interface eth1/1 switchport trunk allow vlan 1 - 4		interface eth1/9 switchport access vlan 2
22		interface eth1/4 switchport trunk allow vlan 1 - 4		interface eth1/11 switchport access vlan 2

- Configure Switches within a Network Policy:
 - Device Templates:
 - You need to determine if the configuration was established using one or more methods: Classic GUI, Sup-CLI, local CLI
 - Determine if the configuration is consistent across devices by reviewing the templates, GUI configuration, and/or CLI running-config
 - Build a template that meets the requirements for the majority of devices
 - Pick a switch in XIQ to begin validating/changing the configuration:
 - At this point, the switch is still operating and communicating with Classic
 - Filter the Device list > Edge Switch to only view switches in XIQ
 - 
 - Click on the hostname > Configure >
 - Device Configuration:
 - Add SNMP Location if applicable
 - Assign Network Policy if not already done so
 - Verify your template was auto-selected
 - Press **Save Configuration** button
 - Port Configuration:
 - While reviewing Classic & your running-config make any GUI changes that deviate from the template
 - Press **Save Configuration** button
 - Close modal window
 - Click on the orange audit mismatch icon
 - Switch to **Complete** tab > Review this configuration against the current running-configuration



Update Certificate for SR2200 & SR2300 Series Switches

A change of certificate occurred on October 21, 2019.

The certificate is required for secure SSL communication between ExtremeCloud IQ and Extreme-Aerohive SR2200- and SR2300-series, and Dell EMC switches. ExtremeCloud IQ automatically updates devices that are connected and managed by ExtremeCloud IQ but cannot update devices that are disconnected or unmanaged, such as those in stock or storage. The old certificate is expired and no longer available.

Devices that have not connected to ExtremeCloud IQ can not receive the new certificate automatically (because ExtremeCloud IQ does not allow connections from devices without valid certificates) and require manual intervention afterward. For information regarding how to update IQAgent (formerly called HiveAgent) and the certificate. Checking the status of the switch results in a Peer certificate error:

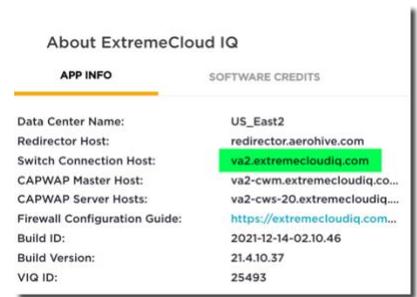
```
(AH-Switch) #show hivemanager status
.....
HiveAgent Status..... CONTACTING REDIRECTOR
HiveAgent Server Certificate Info..... Peer certificate cannot be authenticated
with given CA certificates
HiveAgent Version..... 1.1.29.0
HiveAgent Debug..... ON
HiveAgent Source Interface..... DEFAULT
HiveAgent HTTP Proxy..... -
.....
HiveAgent Association Method..... REDIRECTOR
HiveAgent Association Url..... -
HiveAgent Poll URL..... -
HiveAgent Redirector FQDN..... cloud-rd.aerohive.com
HiveAgent Redirector Response..... Peer certificate cannot be authenticated
with given CA certificates(60)
.....
```

Navigate in XIQ > mouse hover over your name in the top right corner > About

Take note of the Switch Connection Host e.g. va2.extremecloudiq.com

Console or SSH into the SR switch and run these commands:

```
application stop hiveagent  
  
hivemanager address <enter Switch Connection Host name>  
  
application start hiveagent  
  
show hivemanager status  
^^^ You can repeat this last command until you get a Success status
```



About ExtremeCloud IQ	
APP INFO	SOFTWARE CREDITS
Data Center Name:	US_East2
Redirector Host:	redirector.aerohive.com
Switch Connection Host:	va2.extremecloudiq.com
CAPWAP Master Host:	va2-cwm.extremecloudiq.co...
CAPWAP Server Hosts:	va2-cws-20.extremecloudiq...
Firewall Configuration Guide:	https://extremecloudiq.com...
Build ID:	2021-12-14-02.10.46
Build Version:	21.4.10.37
VIQ ID:	25493

Check XIQ and the switch will connect, shows a date/time stamp as well as report its firmware version.

There you have it. A simple way to update the certificate so the switch can communicate with XIQ. Much easier than manually transferring files to the switch.

Migrating a Cloud Virtual Gateway (CVG) & Branch Routers (BR#) Preparation

A few things to note before getting started:

- CVG hardware is not compatible and should be replaced by the VPN Gateway Virtual Appliance (VGVA) or the XR600 physical router which can be a tunnel terminator
- SR2000 & SR2100 series switches were capable of being a router and are not supported in the XIQ GUI interface. These may be migrated using a combination of GUI and S-CLI.
- Export the configuration of the tunnel terminators to your spreadsheet along with a branch router from every network policy that has BR's assigned:
 - Show run
 - Show ip route
 - Show arp
- Create a new VGVA instance and configure XIQ side by side adjacent to your working production network. Decommission the CVGs after the branch routers have been moved. This minimizes downtime.
- Be methodical for a successful project

Classic Interface Migration Steps

Change CAPWAP Primary and Backup Server Target

Step one is to tell the device to wipe its current CAPWAP IP address and replace it with redirector.aerohive.com. You may use your new XIQ VA IP address for on-prem deployments. This can be done on a single device or by multi-editing.

Menu: Configuration > Devices > All Devices

Single Device:

1. Click the device Hostname
2. Expand **Credentials** section
3. Press + icon to create IP object via hostname
(Only need to do this one time)
4. Choose: Host Name
5. Name object: redirector.aerohive.com
6. Enter host name: redirector.aerohive.com
7. Press **Save** button
8. Press down arrow
9. Select: redirector.aerohive.com object
10. Scroll up and press **Save** button

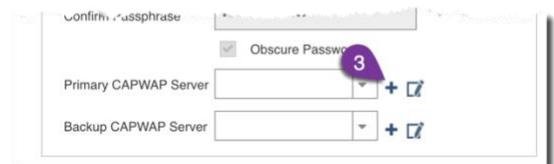


Audit	Host Name	Device Model
<input type="checkbox"/>	AH-d2f200	AP250
<input type="checkbox"/>	AH-43c7c0	AP250
<input type="checkbox"/>	San-Flo-0089	AP150W



2 Credentials

Root Admin Configuration

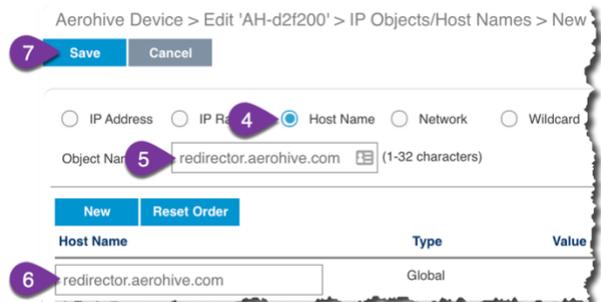


Confirm passphrase

Obscure Password

Primary CAPWAP Server + [icon]

Backup CAPWAP Server + [icon]



Aerohive Device > Edit 'AH-d2f200' > IP Objects/Host Names > New

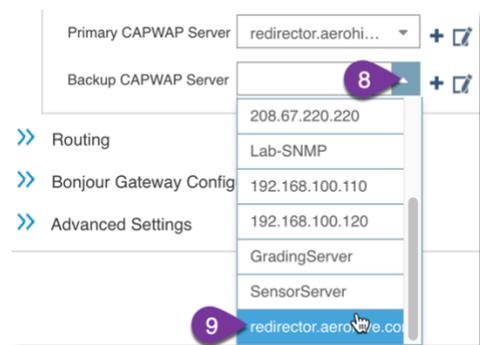
7 Save Cancel

IP Address IP Range Host Name Network Wildcard

Object Name 5 redirector.aerohive.com (1-32 characters)

New Reset Order

Host Name	Type	Value
6 redirector.aerohive.com	Global	

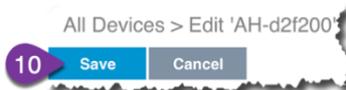


Primary CAPWAP Server redirector.aerohi... + [icon]

Backup CAPWAP Server + [icon]

8

- >> Routing
- >> Bonjour Gateway Config
- >> Advanced Settings
- 208.67.220.220
- Lab-SNMP
- 192.168.100.110
- 192.168.100.120
- GradingServer
- SensorServer
- 9 redirector.aerohive.com

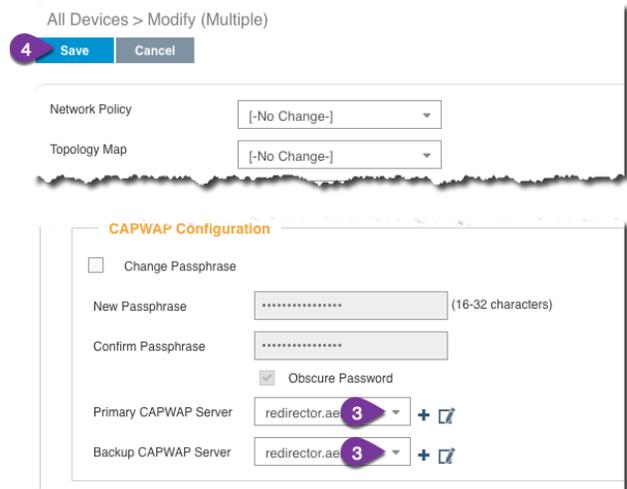
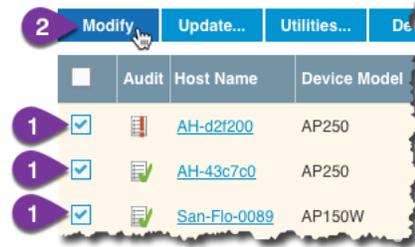


All Devices > Edit 'AH-d2f200'

10 Save Cancel

Multiple Devices:

1. Checkmark one or more devices
2. Press **Modify** button
- Expand Credentials section
3. Change both CAPWAP Servers to *redirector.aerohive.com* or your local XIQ VA IP address
4. Press **Save** button



Update Classic Devices to Make the Move to XIQ

Now that your CAPWAP settings are set in Classic you can now push an update to one or more devices.

1. Checkbox the target Devices(s)
2. Press Update... > Update Devices
3. Checkbox: Perform a complete...



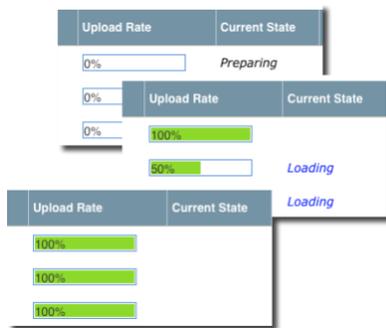
4. HiveOS – choose **Don't Upgrade**

5. Press **Update** button

6. Choose Auto reboot

7. Press OK

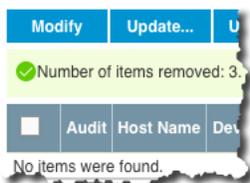
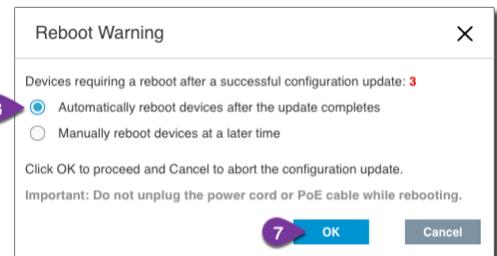
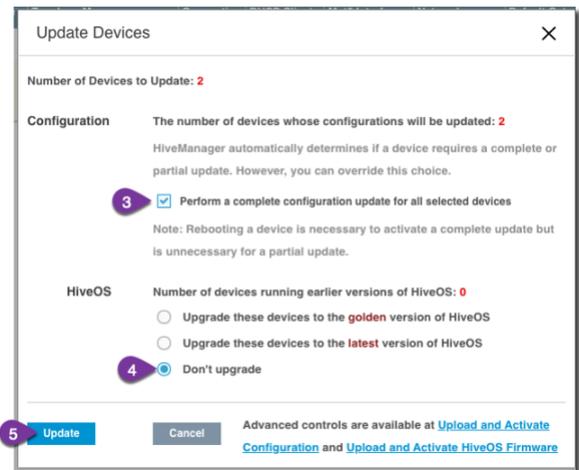
Wait for 100%



8. Go back to device list: Checkbox the same device(s)

9. Press Device Inventory > Remove (Only req'd for Cloud)

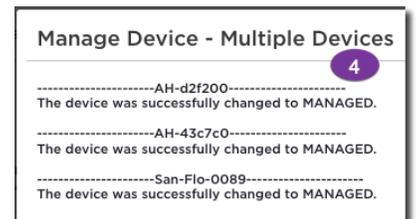
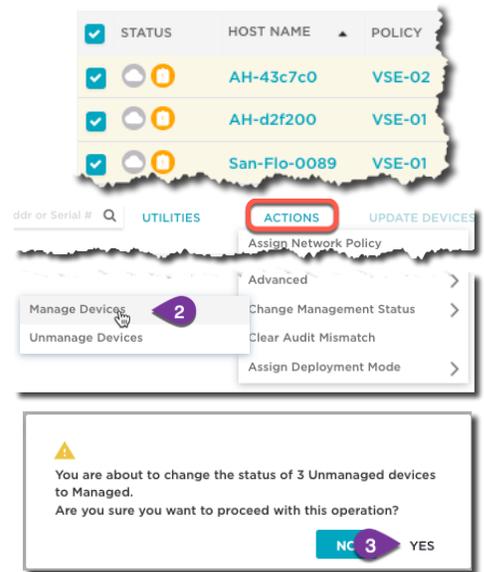
10. Choose: Keep Existing settings > Pres **Yes** button



XIQ Interface Migration Steps

Menu: Manage > Devices

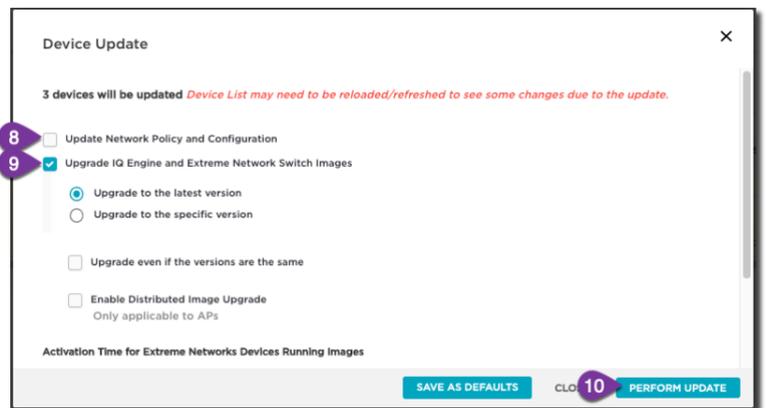
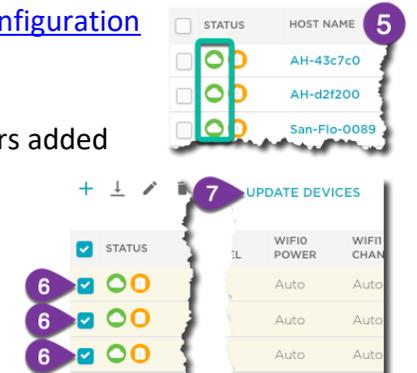
1. Checkbox the AP in XIQ that you just removed in Classic
2. Press **Actions** button > Change Management Status > Manage Devices
3. Press **Yes** button to proceed with the operation
4. You want to see success messages for every device. If not, verify the device was properly removed from Classic. Press OK to close the popup.
5. Wait for the grey cloud to turn green (a connected status meaning CAPWAP has been established)



Notes:

- If your devices are not checking in go back and review this section: [Device IP Discovery](#). Your device might be checking in with a local Classic VA. Did you confirm your Firewall rules are set? [Firewall Configuration Guide](#)
- Your devices need to be manually updated. Only new serial numbers added are auto-updated upon checking into XIQ.

6. Checkbox the device(s)
7. Press **Update Devices** button
8. Uncheck: Update Network Policy and Configuration
9. Checkmark: Update IQ Engine...
10. Press **Perform Update** button



Patience is a virtue:

- Wait for the devices to reboot. View the Updated column.
- Refresh table and verify firmware updated
- All is well when the Updated column has a date and time stamp and the cloud is green (connected)



<input type="checkbox"/>	STATUS	HOST NAME	POLICY	UPDATED
<input type="checkbox"/>		AH-43c7c0	VSE-02	2022-01-05 17:49:51
<input type="checkbox"/>		AH-d2f200	VSE-01	2022-01-05 17:49:36
<input type="checkbox"/>		San-Flo-0089	VSE-01	2022-01-05 17:51:12

Now you will update the configuration:

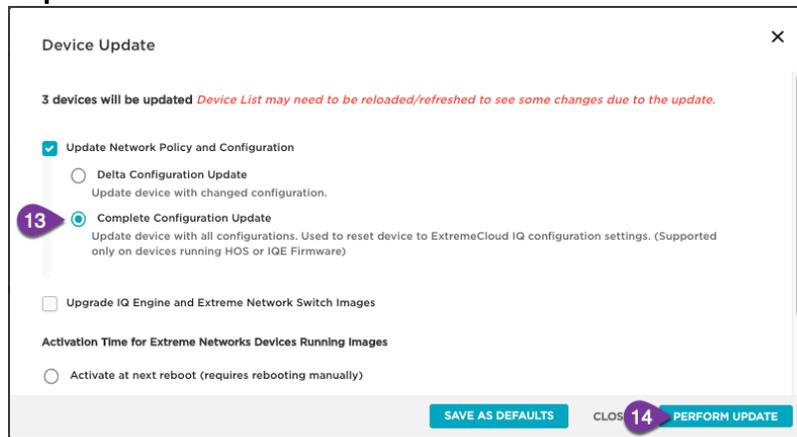
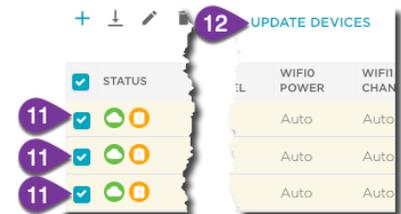
- Verify all your devices are assigned a Policy (see column)

11. Checkbox the same devices(s)

12. Press Update Devices button

13. Always choose **Complete Configuration Update** for the first upload

14. Press **Perform Update** button



- All is well if you see a green cloud and green clipboard along with a date and time stamp under Updated Column. Test test test..., repeat.

<input type="checkbox"/>	STATUS	HOST NAME	UPDATED
<input type="checkbox"/>		AH-43c7c0	2022-01-05 18:00:50
<input type="checkbox"/>		AH-d2f200	2022-01-05 18:00:50
<input type="checkbox"/>		San-Flo-0089	2022-01-05 18:01:42

Client Roaming Between HM Classic and XIQ APs

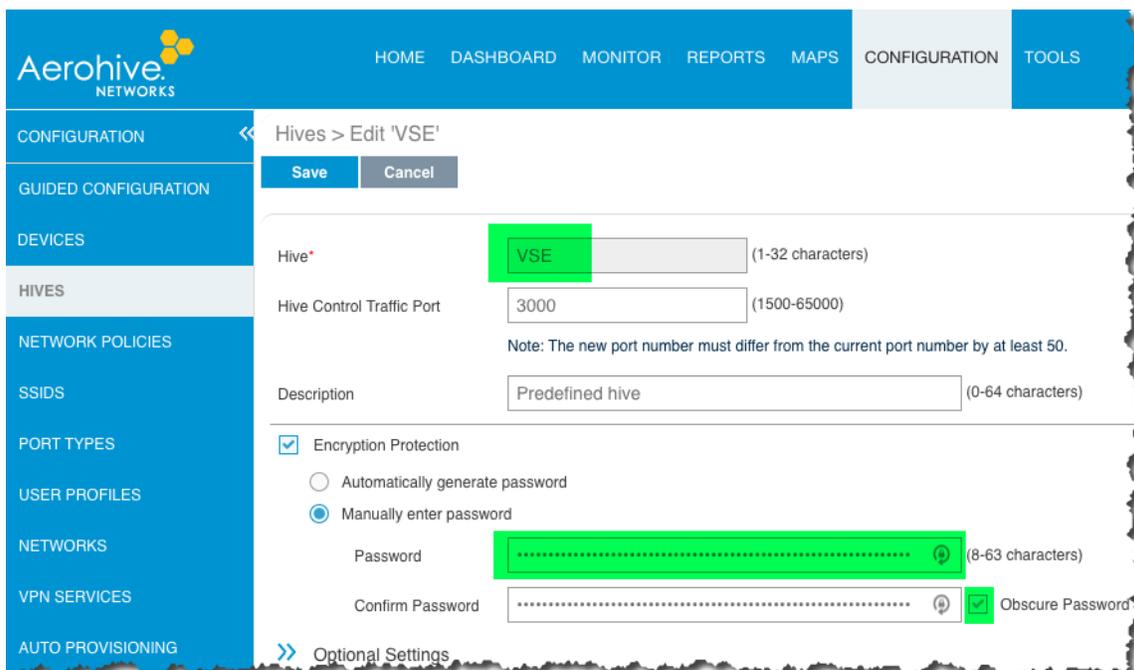
As you plan your schedule to migrate access points from Classic to XIQ, you may find a situation where you must have a mix of Classic and XIQ APs in the same area. Clients need to be able to roam between the two platforms.

First, let's understand how the APs communicate with each other and what is transferred.

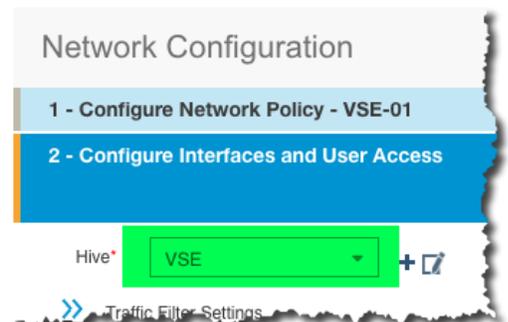
The Hive name and encryption password must match between both platforms so the APs can exchange client information on the LAN:

- Pairwise Master Key (PMK), MAC, and User Profile assignment

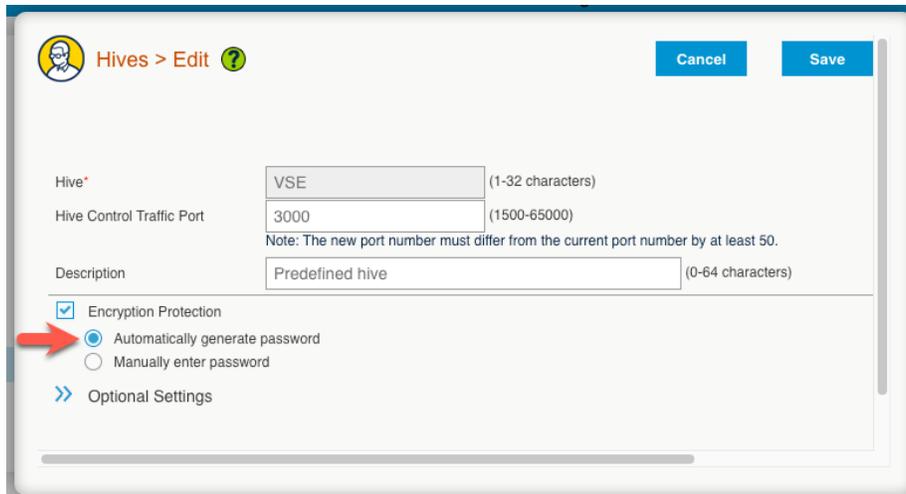
Classic Menu: Configuration > HIVES (lists all configured Hives)



Classic Menu: Configuration > edit Network Policy > Additional Settings: Edit > Hive: <drop down field> (Hive assignment)



Classic: If your Hive: Encryption Protection is set to *Automatically generate password*. You will need to change to *Manually enter password*, generate a secure 63-character password, and push out a configuration change to your Classic APs.

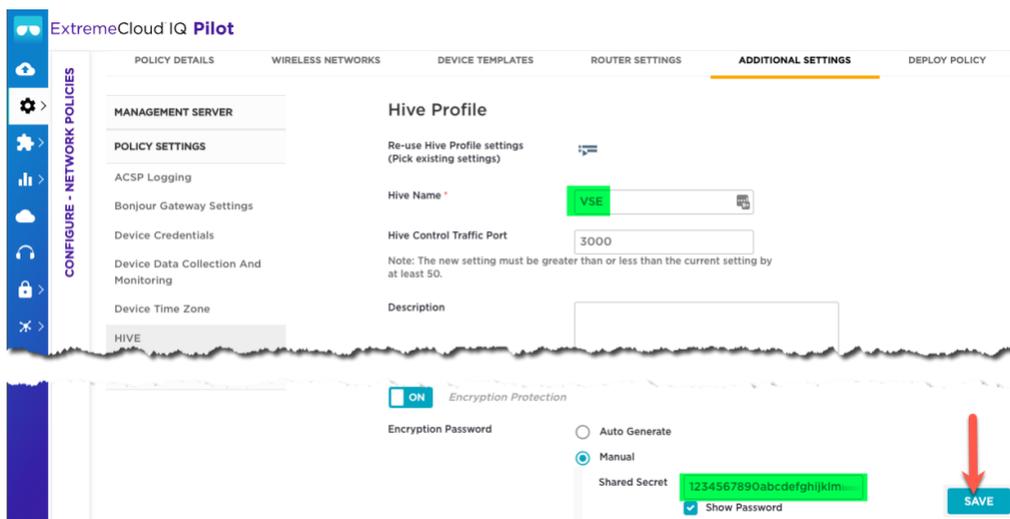


Copy that password to be used in XIQ:



Alternative: You could copy the XIQ Hive password and paste it into the Classic Hive password field.

XIQ Menu: Configure > Network Policies > edit your policy > Additional Settings > Policy Settings > HIVE



Scripts

Create Location, Building, & Floor Objects

Objectives:

- Expedite creating locations, buildings, and floors for your organization if you're missing any
- Fix any Location objects with maps and devices on them since XIQ does not allow this
 - **IMPORTANT:** Devices must be assigned to floor objects in XIQ but Classic GUI allowed devices to be placed on Location objects. After you take a backup and import into XIQ, the devices that are on location objects are brought over but must be fixed after the fact.

STEP 1

- Your Classic backup should've been imported before this point
- This first script creates your Location, Buildings, and Floors referencing a CSV file. XIQ requires devices to be placed on floor objects. This allows XIQ to properly gather, store and present ML data.
- Download Files (https://github.com/timjsmith24/XIQ_Locations_CSV_Import),
 - Press Code button > Download ZIP
 - *XIQ-Move-Devices-To-Floor-Object.py*
 - *Location-Building-Floor_Builder.py*
 - *Location-Building-Floor_Tree.csv*
- Extract the zip and place all files in the same folder

STEP 2a – MacOSX BigSur

- Open Terminal app
- Change directory to your file location, this guide uses the downloads folder: `CD \downloads`
 - Verify your files exist in this directory: `ls`
- Check your installed Python version: `python3 --version`
 - Must have a minimum version of 3.8.X installed, 3.10 not supported
 - Install Command Line Developer Tools when prompted
 - Run this once more to confirm: `python3 --version`
- Check your Pip version: `pip3 --version`
 - If you see an Import Error; repair the installation of PIP: (we believe this is a bug by Apple)
`curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py && python3 get-pip.py`
 - Install required packages: `pip3 install -r requirements.txt`
- Running python commands on a Mac: `python3 <file-name.py>`

STEP 2b – Windows 10 Pro x64

- Search in the Windows Store for Python 3.9 and install it
 - 3.10+ is NOT supported so choose v3.9
 - You will be prompted to login with Microsoft credentials
 - Next window begins to download and install
 - Close MS store window after installation



- Launch **Windows PowerShell**, Run as an Administrator
- Change your directory to be the path where your files are stored: `CD C:\Users\mike\Downloads`
 - Verify your files exist in this directory: `ls`
 - Install required packages: `pip3 install -r requirements.txt`
 - *Requests* and *Pandas* packages will download and install
- Running python commands in Windows: `python3.exe .\<file-name.py>`
 - If you receive an *Error creating building in XIQ - HTTP Status Code: 401 <Response [401]>*, try entering your credentials by typing them in instead of using copy and paste. What happens in the background is the credentials are passed to XIQ with an invalid password.

STEP 3

- Open *Location-Building-Floor_Tree.csv* in a raw text editor, Excel may have reformatting problems upon saving.

- Populate the CSV as shown in the example below for your organization: (image legible on PDF)

```
loc_name,sub_loc_1_name(if necessary),sub_loc_2_name(if necessary),building_name,address,floor_name,environment,attenuation,measurement,height,map_width,map_height,map_name
LocationCountry1,LocationState1,LocationSite1,Loc1Bldg1,3988 Las Vegas Blvd Las Vegas NV 89119,Floor 1,OFFICE,15,FEET,9,50,50,
LocationState2,LocationSite2,,Loc2Bldg1,3988 Las Vegas Blvd Las Vegas NV 89119,Floor 2,OFFICE,15,FEET,9,50,50,
LocationSite3,,Loc3Bldg1,1010 J Street Modesto CA,Floor 1,OFFICE,15,FEET,9,500,386.33,Casino Floor_v3.png
LocationSite3,,Loc3Bldg1,1010 J Street Modesto CA,Floor 2,OFFICE,15,FEET,9,50,50,
```

- **Loc_name** (required) = Enter location object name
- **Sub_loc_1_name** (optional) = Nested location object (Location > Location)
- **Sub_loc_2_name** (optional) = Nested location objects (Location > Location > Location)
- **Building_name** = Enter building object name
- **Address** = Enter building address that will be applied to the building object
- **Floor_name** = Enter a floor name. If multiple floors, enter a unique floor name along with the same location & building names

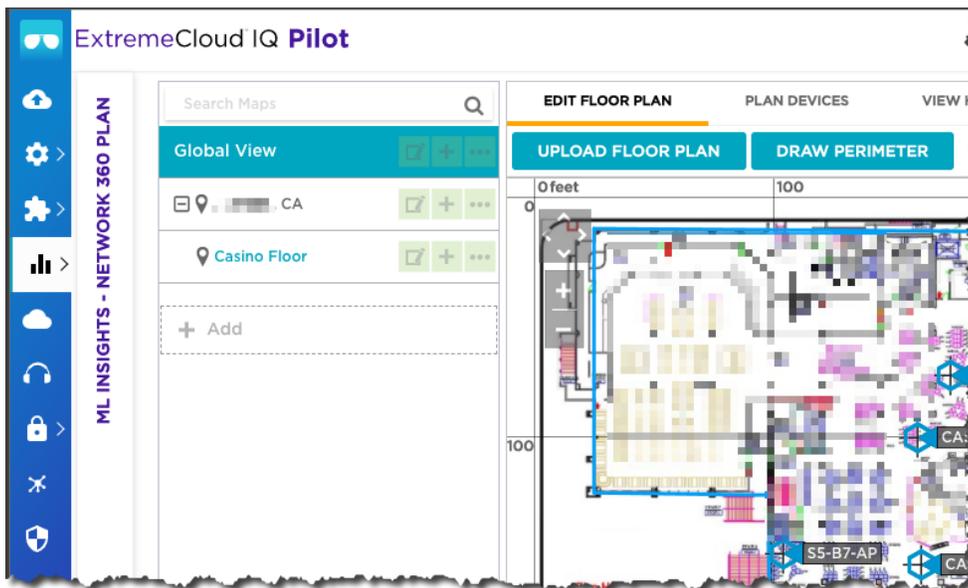
- **Environment** = This verbiage is specific, use *OFFICE* and change in XIQ after creation if desired
- **Attenuation** = Enter a value for dB loss between floor (default: 15)
- **Measurement** = **FEET** or **METERS**
- **Height** = Enter an AP placement height per floor
- **Map_width** = This value will be acquired later, use any value for now
- **Map_height** = This value will be acquired later, use any value for now
- **Map_name** = This value will be acquired later, leave blank for now
- Do not add a comma to the end of a row if you're using a map name

*** Do not run the script at this time ***

Fix Map & Devices on Location Objects in XIQ

STEP 4

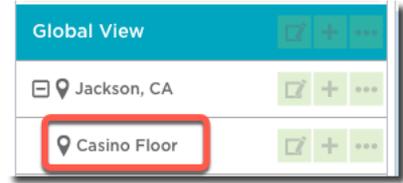
Do you have maps assigned to a Location object as shown below? Location objects have a pin drop/teardrop icon next to the name.



If so, complete these steps before running any scripts. If not, you may skip this step/section and create your hierarchy.

Note: Walls objects are not moved. APIs don't exist today for these objects.

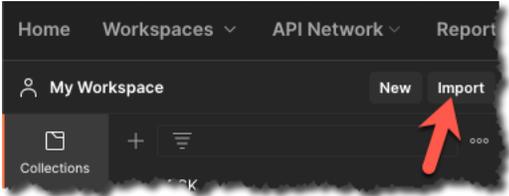
- First, locate the location object that contains a map with devices
- Click on the (e.g. Casino Floor) location object (where your floor plan map is with APs) and copy the numeric value in the URL

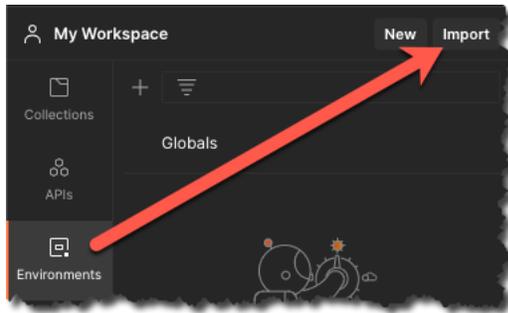


<https://rdc.extremecloudiq.com/#/plan/723491536096601/overview>

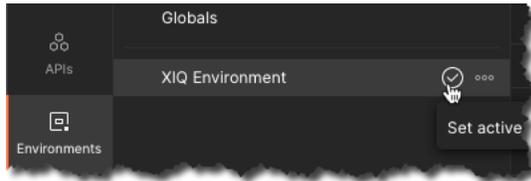
Copy: [723491536096601](#)

STEP 5

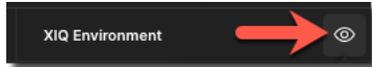
- Download the free Postman app here: <https://www.postman.com/downloads/>
- You'll use Postman app to grab the map name and size
 - Download our XIQ Postman Framework here: https://github.com/extremenetworks/ExtremeCloudIQ-APIs/blob/main/XIQ%20APIv2%20New%20Framework.postman_collection_May2021.json
 - Title: XIQ APIv2 New Framework.postman_collection_May2021.json
 - Simplest way to download the file is to press the Raw button (top right corner of the code window)
 - Save Page As > XIQ APIv2 New Framework.postman_collection_May2021.json
 - Import framework into Postman
 - Collections menu (left column)
 - Next to My Workspace press Import button
 
 - Complete importing the framework
 - Download our XIQ Postman Environment Variables here: https://github.com/extremenetworks/ExtremeCloudIQ-APIs/blob/main/XIQ%20Environment.postman_environment_May2021.json
 - Simplest way to download the file is to press the Raw button (top right corner of the code window)
 - Save Page As > XIQ Environment.postman_environment_May2021.json
 - Import environment variable into Postman
 - Environments menu (left column)
 - Press Import button



- Complete importing the environment variable
- Set the XIQ Environment Active > mouse hover over the checkmark area and click



- Menu: XIQ APIv2 New Framework_MAY2021 > Authentication > Login Basic Authentication
- Click Eye icon (top right corner) next to XIQ Environment

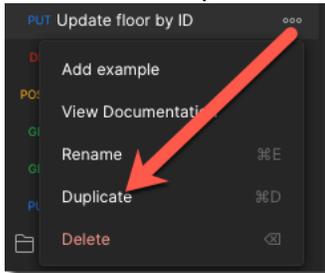


- Edit user name and password in initial and current fields. These are your XIQ credentials of a local account, not an external admin.
- Press Save then close the Environment Variable tab

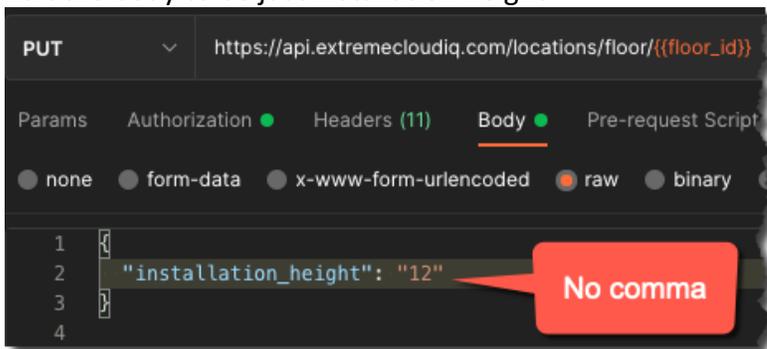
XIQ Environment		
VARIABLE	INITIAL VALUE	CURRENT VALUE
username	mik [redacted] @gmail.com	mik [redacted] @gmail.com
password	GD8 [redacted] qOM	GD8 [redacted] .OM

- Menu: XIQ APIv2 New Framework_MAY2021 > Authentication > Login Basic Authentication
- Press Send
- Authenticates using your XIQ credentials and you should receive an access_token in the body which is stored for you in the Environment Variables: *jwttoken*
- Click Eye icon (top right corner)
- Edit **floor_id** field in initial and current fields of the Location ID object: **723491536096601**
- Press Save then close the Environment Variable tab
- Menu: XIQ APIv2 New Framework_MAY2021 > Configuration - Location > PUT-Update floor by ID
- Switch to the Body sub-tab under the PUT : API URL bar

- Click on the ellipses and Duplicate the object:



- PUT – Get floor info by ID:
- Edit the body to be just installation height



- Press Save button
- Press Send button
- Output → → →



- Open the *Location-Building-Floor_Tree.csv* file in a raw text editor
- Enter the information obtained in Postman for your new Location, Building, Floor

`s,floor_name,environment,attenuation,measurement_height,m
s,MEASUREMENT_UNIT_FEET,9,500,386.33,Casino Floor_v3.png`

- Repeat for all other locations that contain a map and devices
- It's okay that a floor does not have a floor plan image. Adding an image name is optional.

STEP 6

It's time to create your hierarchy then you can move devices.

Run script: `python3 Location-Building-Floor_Builder.py`

- Enter your XIQ email address
- Enter your XIQ password
- Enter the CSV file name including the extension: *Location-Building-Floor_Tree.csv*

Navigate XIQ Menu: ML Insights > Network 360 Plan and review the results. If you do not see any changes refresh your browser.

Verify the floor plan map that was originally in your Location object is now on your new floor object as shown in the example → → →

The next step is to move your devices from the old Location object to the new Floor object.

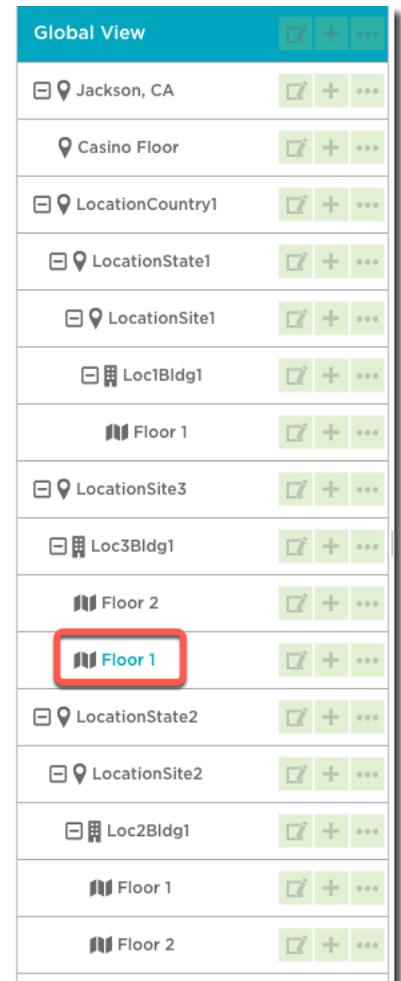
- Get your (e.g. Casino Floor) location object (where your floor plan map is) ready, Copy: [723491536096601](#)
- Click on the (e.g. Floor 1) Floor object (where your devices will move to) and copy the numeric value in the URL

<https://rdc.extremecloudiq.com/#/plan/723491536096702/overview>

Copy: [723491536096702](#)

Run script: `python3 XIQ-Move-Devices-To-Floor-Object.py`

- Enter your email you use to login XIQ with:
- Enter your password:
- Enter the location ID where the devices are currently: [723491536096601](#)
- Enter the floor ID where the devices will be moved to: [723491536096702](#)



REPEAT for each location. It's important to do this methodically. Control the variables for a successful migration.

STEP 7

Verify your maps and devices have moved.

- Click on the old Location object and verify all devices have been removed
- Click on the new Floor object and verify the map and devices are present

WARNING!!! Wall objects can't be moved programmatically at this time. Manually recreate perimeter and walls before the cleanup stage.

- Clean up by deleting the old location object(s) since this is a potentially corrupt object in XIQ
 - If there are objects below this location you must either delete them or move them before XIQ will allow you to delete the old location object from the database

Admire your finished work knowing you saved time and effort by using Python and API calls.

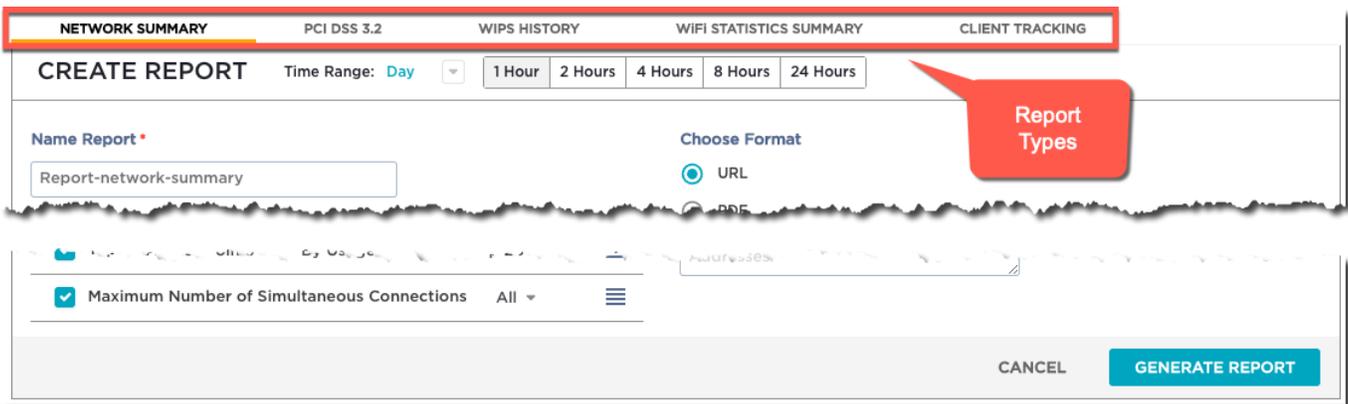


Reports

Review reports configured in HM Classic. Menu: Reports

Please note, reporting features in HM Classic are far more granular than what XIQ provides. There's no direct migration from one report to another.

XIQ Menu: Manage > Reports



WiFi Statistics Summary offers a 30-day raw data dump you can use Excel to develop reports from.

Library customers that rely upon unique devices broken down per location can take advantage of custom scripts written specifically for this purpose by our Solutions Architect team.

- YouTube video link: <https://www.youtube.com/watch?v=m-KPitYfmfY>
 - Overview:
 - In XIQ (Menu: Manage > Reports) run the WiFi Statistics Summary report (30 days of data)
 - Recommend you set this up on a monthly recurrence or you will lose the ability to report the data regardless of what RDC your VIQ is on. The report is limited to 30 days of data and is not adjustable.
 - Download the scripts from GitHub repository: https://github.com/timjsmith24/XIQ_Client_Report_CSV
 - Install the necessary software & extensions for Python (Windows or Mac)
 - Run the script
 - Open the XLSX file for review and print
- All devices **must** be placed on a floor within a Building within a Location
 - All APs that are not assigned to a floor will not generate in the raw data export
 - Simply fix the assignment and re-export to fix the data. The data exists in the back end, just needs an assignment.

Access Point Country Codes Verification

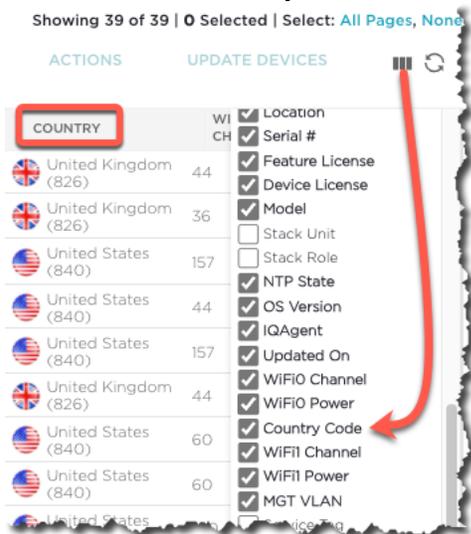
This isn't specifically a migration topic but something to be aware of. When you migrate your APs from Classic to XIQ you should verify that your country codes are accurate. I encountered a situation where a customer had no idea how three of their 39 access points were using World-UK Country Code 826 and not FCC Country Code 840.

AP's purchased before the new World Side SKU are geographic region-specific. To change country codes you must reach out to GTAC and see if they're willing to change the code. This requires CLI access with specific passwords and commands. This is a grey area. Sometimes changing is against regulations, sometimes it's not.

ExtremeCloud IQ:

Menu: Manage > Devices

- Add a column **Country Code**



Troubleshooting

A list of things to consider:

- Compare two CLI outputs to validate configuration, <https://www.diffchecker.com/>
- Physically reset the AP and try again...
- Get your console cable ready. The newer AP's require a Micro-USB cable with the proper hardware embedded. Part/SKU #: ACC-WIFI-MICRO-USB
<https://extremeportal.force.com/ExtrArticleDetail?an=000079289&q=micro%20usb>
- Have you addressed the new Firewall Rules in XIQ?
- Confirm the device is showing as “managed” in XIQ
 - If marked as “unmanaged”, correct it and wait up to 10 minutes for the device to connect
- Reverse the process and start the migration process over, perhaps you missed a step
- Confirm that DNS is correct and working, must be able to resolve URL's
- Confirm that you set the CAPWAP servers to point to the redirector
- Attempt to ping the device from another device on the network, like another AP.

You should consider calling support at this point!

Troubleshooting – Steps to take if the device never connects to XIQ

Here's a great in-depth Advanced CAPWAP troubleshooting article:

<https://extremeportal.force.com/ExtrArticleDetail?an=000057794&q=capwap%20timeout>

- a. Confirm the device is showing as “managed” in XIQ
 - I. Select the column picker in XIQ and add the managed column.
 - II. If it's not, change it to “managed”
 - III. If it's already “managed”, move to the next step.
- b. Change the device management status to “unmanaged” which releases the serial number
- c. Copy the serial # from XIQ and onboard the device in Classic again
 - I. Typically, the AP will be connected to the redirector waiting for the URL of its instance
 - II. Once the AP has connected back to HiveManager
 - a. confirm that DNS is correct and working
 - b. confirm that you set the CAPWAP servers to point to the redirector or the local IQVA address
 - c. attempt to migrate the device again
- d. Attempt to ping the device from another device on the network, like another AP.

- I. Use either HiveManager or XIQ to gain CLI access to an AP that is online to test ping to the stranded device
- II. If you can ping the stranded device, then run the following commands to gain CLI access to the device via SSH to troubleshoot
 - a. `#exec ssh server <ip of stranded ap> user admin //enter`
 - b. `#sho capwap client`
 1. confirm that your CAPWAP server IP starts with 34.X.X.X or 3.X.X.X. If the IP address starts with 54.X.X.X the device is connected to redirector and safe
 2. confirm that your HiveManager Primary Name matches what you see in XIQ.
 1. Check “About ExtremeCloud IQ” to find your CAPWAP Master host URL
 3. manually configure the Primary Server Name
 4. run `#save config`
 5. run `#no capwap client enable //to stop the capwap service` run `#capwap client enable //to start the capwap service`
- e. If your device CAPWAP Primary Server is trying to connect to Classic then you may disable the L2 discovery mechanism: `#no capw client discovery method broadcast`

```
Global Technical Assistance Center
(GTAC) for Immediate Support
Phone: 1-800-998-2408 (toll-free in
U.S. and Canada) or +1 408-579-2826.
For the support phone number in your
country,
visit: www.extremenetworks.com/
support/contact
```

Call to Action

While this guide has covered many aspects of the migration process in great detail, it may miss a few situations. Please contribute any scenarios you've encountered to keep this guide growing until every last Classic system is migrated. Feel free to reach out to me below.

End Guide

Shout-outs go out to the entire Solutions Architect team including Franco Gobbetti, Geoff Mason, Gordon Jennings, and Mike Eversole. Also, our API Python guru Tim Smith, CWNE building serious time-saving scripts.

Good luck and be safe out there.

Mike Rieben, Solutions Architect (Western US)

mrieben@extremenetworks.com

<https://www.linkedin.com/in/mikerieben/>