# Qualys (API Driven) Subscription Migration

## *Vulnerability Management & Policy Compliance v 0.9.1*

## Contents

## Objectives

- To affect the migration of a subscription to a separate subscription using only API calls where possible
- Provide logic processing rules for transformation of output data into input data
- Determine any manual interventions or manually submitted data and provide for their automation
- Focus is to “forklift” the subscription between platforms. Although a few “best practices” are added to improve during the move.

## Overview

API calls can be made to export a range of subscription data and settings and, in combination with off-platform processing to manipulate output data into input data, can be used to import that same data into a new subscription. However, this API coverage is incomplete and there exists several data that must be replicated manually
The key manual steps from are as follows
(From within the user interface of the Qualys application)

1. Manually pull and replicate the licensed IPs and domains
2. Manually pull and replicate the asset groups, tags, options profiles, report templates, authentication records, etc., from the old subscription
3. Manually pull and replicate the scan schedules, targets, etc.
4. Manually pull and replicate the users, SAML integrations, etc.
5. capture the reports they need in their internal business records
6. If there are PCI merchant accounts linked to individual; Qualys VM accounts, each user account must be unlinked by each user from within their own Qualys user interface
7. If scanner appliances are being migrated, the customer should contact support, via telephone or by creating a Support ticket, when they are ready to have the appliances disassociated/ unbound from their current user accounts. Please be sure to specify the serial number of the appliance and the username they are currently bound to
8. Once the appliance(s) is unbound, it’s free to be activated on another subscription in the same SOC. For migrations between SOCs, physical appliances will need to be replaced by Qualys.

### Pre-Requisites

Authentication Records cannot, by design, be fully exported from the Qualys platform. When exporting an Authentication Record the ‘secret’ information (password, secret key, etc.) is not included in the output. It is therefore necessary to provide this information separately. In order to correctly allocate this information to the appropriate Authentication Record, each new credential record provided must also include the name of the Authentication Record to which it relates.

Once compiled the data should be encrypted using AES256 with an appropriately complex passphrase. The data will remain encrypted at rest and will be decrypted by the script which manages this aspect of the migration.

It is key to understand that the password is not part of the export / import.

## Task Structure

In order to complete the manual steps provided in the Outline various component tasks must be completed such as the Export and Import of Asset Group data, Authentication Records, etc. These component tasks are defined as follows

- Core Tasks
- Processing Tasks
- Input Tasks

### Core Tasks

Core tasks are the component tasks for each of the manual steps defined above. For example, step 2 covers pulling several items for replication into the target subscription. The core tasks associated with this step would cover the individual tasks associated with that activity, such as pulling asset groups, pulling option profiles, etc. Almost all of these core tasks has an associated export and import task component and zero or more processing or input tasks.

| | |
|---|---|
| Subscription configuration | Report Templates |
| Users | Authentication Records |
| Networks | Search Lists |
| IPs | IPv6 Mappings |
| Domains | Compliance Policies |
| Asset Groups | Remediation Rules |
| Asset Tags | Scanner Appliances |
| Option Profiles | Scan Schedules |

**NOTE:** Remediation rules cannot be exported or created with the API.
This list is not prioritized or ordered.

### Processing Tasks

Processing tasks are the component tasks related to core tasks. They take the output from one core task component (e.g. List Asset Groups) and turn it into the input of another (e.g. Create Asset Groups). Processing tasks can also take input from manual sources and use it to produce output data for certain tasks (e.g. Create Unix Authentication Record)

### Input Tasks

Input tasks are the component tasks which identify, handle and process externally provided data where that data cannot be obtained through the Qualys APIs. An example of this is found

in step 2 where authentication records are pulled from the platform. Authentication records do not disclose private key material or passwords, so this information must be provided manually and in formatted in such a way as to allow processing by a Processing task.

## Clean up prior to migration

If features like Cloud Agents and or Agentless tracking are used, these need to be cleaned up PRIOR to migrating data and decommissioning the old subscription.

There are basically 2 ways to do this:

1) Remove ANY and all cloud agents that are currently connecting to the platform.
    a. Either thru the Clud Agent application on the platform and remove all the agents thru a "uninstall job"
    b. Or, follow the documented Uninstall process from the Cloud agent documents.

2) Secondly, Use the "clean up" function on the CURRENT Qualys platform.
    a. This can be found on Scan → Setup → Agentless Tracking → CLEANUP.
    b. This clean up needs to be done, to avoid conflict with the new subscription.
    c. It can also be done "manually" thru a SCCM / Puppet / etc / etc script to clean up the registry setting on this hive entry:
        i. HLKM\SOFTWARE\Qualys\HostID
        ii. /etc (unless changed by customer) for Unix based systems.
    d. It is important to understand that, once the cleanup option has been enabled, this will remain ON until the Agentless tracking option is accepted again. The Cleanup function is performed when we authenticate to an asset during a VM scan and Agentless Tracking is enabled on the Authentication Record
    e.
        i. So as long as the clean-up is not "undone" then we will continue to clean up the agentless tracking artefact on every scan we do with authentication and the Agentless tracking checkbox enabled.

## Core Task Breakdown

### Subscription Configuration

The subscription configuration covers all configurations made in the various Setup tabs within each VM section, for example User Setup options, including subscription-wide password security settings.
There is a separate Qualys Subscription API which covers the export and import of that data without any associated processing or input task components

### Users

All user configurations need to be exported including Business Units and their configurations
User Data is defined as

- Contact Information
- User Role
- Assigned Business Unit
- Unit Manager and Manager POC values
- UI Interface Style
- Permissions
- Notification settings

Business Unit data is defined as

- Business Unit Name
- Assigned Asset Groups
- Assigned Scanner Appliances

NOTE: Business Units cannot be exported with the API and must therefore be created manually prior to this task component being executed. This includes Scanner Appliance and Asset Group assignment.

Input Tasks

- List of Business Unit IDs and names
- Mapping of Business Unit IDs, Old to New

Processing Tasks

- Correlate Business Unit from Old to New mapping
- From List Users output and correlated Business Unit IDs, build a list of Create User URLs to create a each new user account

### Networks

Networks have assigned scanner appliances and a name.

WARNING: When adding IP addresses using the API it is not possible to assign them to a Network. They are, by default, added to all defined Networks in a subscription with the Networks feature enabled.
Processing Tasks

- Build list of Create Network URL from List Networks output

**IPs**

WARNING: When adding IP addresses using the API it is not necessary to assign them to a Network. They are, by default, added to all Networks in a subscription with the Networks feature enabled.
IP addresses come in 3 flavors; IP-Tracked, DNS-Tracked and NETBIOS-Tracked.
IP addresses can also be enabled for VM, Policy Compliance and Certview, however Certview IPs should now be added directly within the CertView app and so are out of scope for this process.
Maintaining separate processes will simplify the migration.
Processing Tasks

- For each enabled module and tracking method, obtain the list of IPs from the source subscription
- For each obtained list, construct and execute an Add IPs call in the target subscription

**Domains**

Domains contain only a name and a netblock. API can be used to list all domains, the results from which can be processed by a Processing task to create a list of URLs to re-create them in the target subscription. No input tasks are required.
Processing tasks

- Create a list of Add Domain URLs for each Domain in the List Domains output

**Asset Groups**

Asset groups need to be exported and must include all configurable asset group data. The VMPC API can be used to list all asset groups, the results of which can be processed by a Processing task to produce a set of URLs used to re-create them in the target subscription. One or more Scanner Appliances may be assigned to an Asset Group with one appliance being nominated as the default appliance. Appliances are added by their ID and not their name, therefore an input task is required to provide mapping of source appliance IDs to target appliance IDs is required. Additionally, Networks may be configured in the subscription and an Asset Group assigned to a particular Network. An input task is therefore required to provide mapping of source to target Network IDs so that Asset Groups can be correctly assigned. Location, Department and Function attributes of an Asset Group are not exportable and must be set manually.
Input tasks

- Create a mapping of source appliance ID to target appliance ID

Processing tasks

- Create a list of Add Asset Group URLs from the List Asset Group output

**Asset Tags**

Asset Tags are commonly built in a hierarchy and the API will include that hierarchy in its response to a Search Tags API call. However, the children in this output only contain TagSimple nodes which consist of just the Tag ID and Name. The full tag structure for these tags is included later in the response as a Tag node. Some processing is therefore required, first to remove the system-generated tags and second to reconstruct the hierarchy with full tag structures. Additionally, the child tags listed in the API response are contained within a <list> node, whereas the submission of a tag requires that the child tags be parented to a <set> node. The final step, therefore, is to replace all <list> nodes with <set> nodes.
A tag hierarchy is defined as a series of child tags of any depth, the parent tag for which is a root node. System managed tags are excluded.
Groovy Script support is not enabled in new subscriptions by default. If Groovy Script is used in any Asset Tags, support will need to be added to the target subscription before migration of Asset Tags. This is achieved through a Support or Customer Services case.
No input tasks are required
Processing tasks

- Obtain all Asset Tags configured
- Remove all system-generated Asset Tags (Business Units, Asset Groups, Malware Domain Assets)
- Restructure the Asset Tag hierarchy, replacing TagSimple nodes with the full Tag node structures
- Replace <list> nodes with <set> nodes
- Re-parent Asset Search child tags to a new 'Imported Asset Search Tags' node
- Re-parent Cloud Agent child tags to the existing Cloud Agent tag in the target subscription
- Create each top-level tag, with its full hierarchy, via the Create Tag API call

**Option Profiles**

Option profile exports and imports can be achieved using the Qualys Subscription API without any processing of the output. No processing tasks are required.

**Report Templates**

Report Templates can be exported and imported with the VMPC API. A processing task will be required to create a list of URLs used to re-create the templates in the target subscription.
Processing tasks

- Compile a list of Create Report Template URLs for each template defined in the List Report Templates output

**Authentication Records**

Authentication records are exported from Qualys using the VMPC API but they are incomplete. They do not include the 'secret' portion of the record, commonly the username but often also SSH keys. This is for security reasons, to ensure that the full credentials are not viewable. It is therefore necessary to provide a list of passwords to be used for each authentication record in order for the full record to be recreated in the target subscription.
A list of usernames and passwords is dangerous in any context, and in the increased numbers required for migration exposure of these passwords presents a major security risk. It is therefore required that input file containing the identifier for the authentication record, be that the username or the authentication record name, and the password be provided in encrypted form using AES256 and secured with a passphrase which is to be entered interactively.
A number of processing tasks will be required to decrypt the input file, list the authentication records, correlate the records against the decrypted password input and compile a list of type-specific Create Authentication Record URLs.
Processing tasks

- Decrypt AES256-encrypted input data using passphrase entered by interactive user
- List authentication records, correlate passphrase from input data
- Compile a list of type-specific Create Authentication Record URLs

**Search Lists**

NOTE: Threat Protection RTIs are not included in the exported data when using the API. Any Search Lists which include Threat Protection RTIs should be re-created manually
Search Lists can be exported and imported with the VMPC API. Some processing of the exported output is required to produce input to the Create Search List call.
Processing tasks

- Compile a list of Add Static Search List URLs from the output of List Static Search Lists output
- Compile a list of Add Dynamic Search List URLs from the output of List Dynamic Search Lists output

**IPv6 Mappings**

IPv6 Mappings consist of a ‘special’ IP in the range 0.0.0.0/8 (0.0.0.0 – 0.255.255.255) and a mapping record which maps the IPv6 asset to the IPv4 address. The IPv4 addresses are added to the subscription as ‘normal’ IP addresses so will be recreated when the subscription IPs are migrated. This core task will migrate the mapping records and associate them with a ‘special’ IP.
Processing tasks

- Compile the input POST data for an Add IPv6 Record from the output of List IPv6 Records
- Please ensure you speak with your TAM prior to engaging on this activity to get “extended ipv6 mappings” enabled on the new subscription. This new capability will

automate, and more importantly hide, the mapping in the background allow for a real IPv6 experience in the UI. This process is mention din the document therefore more as a matter of completeness, but in a ideal world should not be “forklifted” from the old to the new subscription. As such, this step is purposely omitted from the table below in the document.

**Compliance Policies**

Compliance policies are exported in XML format individually. A Compliance Policy List call will return the names and IDs of policies which can be used to compile a series of Compliance Policy Export calls to extract all policies. The same list can be re-used to import the policies using a series of Compliance Policy Import calls.
Processing tasks

- Compile a list of policies and Compliance Policy Export URLs from the output of Compliance Policy List
- Compile a list of Compliance Policy Import URLs from the output of Compliance Policy List

**Scanner Appliances**

Scanner appliances cannot be migrated between subscriptions and must be new appliances deployed to the target subscription. These appliances should retain the same name as the original to enable the mapping of origin to target appliances in scan schedules.

**Scan Schedules**

Scan Schedules require scanner appliances to be identified so it is important that appliance names match between origin and target subscriptions.
Schedules can be exported with the List Scan Schedules. The output from List Scan Schedules is in XML however the Create Scan Schedule call is URL encoded with no POST data supported. A processing task will therefore be required to compile a list of Create Scan Schedule URLs from the output of List Scan Schedules.
Processing Tasks

- Compile a list of Create Scheduled Scan URLs from the output of List Scan Schedules

Remediation Policies

IPv6 Mappings

Cloud Connectors

Compliance Reports

## Core Task to API Call Mapping

| Order | Task | API | Origin Call | Target Call |
|---|---|---|---|---|
| 0 | Business units | Manual | | Recreate the BU's from source to target subscription |
| 0 | Networks | VMPC | Network List | Create Network |
| 1 | IPs | VMPC | IP List | Add IPs |
| 2 | Scanner Appliances | VMPC | Scanner Appliance List | Manage Virtual Scanner Appliance (action=create) + Update Physical Scanner Appliance + Scanner Appliance VLANs and Static Routes |
| 3 | Asset Groups | VMPC | Asset Group List | Manage Asset Groups (action=add) |
| 4 | Users | VMPC | User List | Add/Edit User (action=add) |
| 5 | Subscription configuration | Subscription | Export | Import |
| 6 | Asset Tags | AM&T | Search Tags + processing + Get Tag Info | Create Tag |
| 7 | Authentication Records | VMPC | List Authentication Records | Additional Input + Create Authentication Record (type specific) |
| 8 | Search Lists | VMPC | List Static Search Lists + List Dynamic Search Lists | Create Static Search List + Create Dynamic Search List |
| 9 | Option Profiles | Subscription (Documented in VMPC User Guide) | Option Profile Export | Option Profile Import |
| 10 | Report Templates | VMPC | Export | Create |
| 11 | Compliance Policies | VMPC | Compliance Policy - Export | Compliance Policy - Import |
| 12 | Scan Schedules | VMPC | VM Scan Schedules (action=list)<br>PC Scan schedules | VM Scan Schedules (action=create)<br><br>PC Scan Schedules (action=create) |

| Order | Task | API | Origin Call | Target Call |
|---|---|---|---|---|
| | | | (action=list | |
| **13** | **Remediation Rules** | **NONE** | **MANUAL** | **MANUAL** |
| 14 | IPv6 Mappings | VMPC | IPv6 Mapping Record List | Add IPv6 Mapping Records |
| 15 | Domains | VMPC | Domain List | Add/Edit Domain (action=add) |
| 16 | Compliance policies | VMPC | Export Policy | Import policy |
| **17** | **Compliance reports** | **NONE** | **MANUAL** | **Manual copy report template settings, no automated options available.** |
| **18** | **Cloud Connectors** | **AM&T** | **<cloud data connector>, list** | **<cloud data connector>, create** |

# Guidance

## IP addresses / Hosts Assets

Qualys recommends to simply add ALL RFC1918 space to the host asset database thru the webUI.

RFC 1918 ranges are all internally used, and should all be available for “whatever may come” in the future. Also considering the use of more and more cloud services and Qualys agents in “unknown” IP space makes it efficient to just add all RFC 1918 address space to the new subscription.

To do this, just login to the new subscription via the webUI, and go to assets → hosts assets → and add new IP tracked assets here, upon which you enter the CIDR blocks 10.0.0.0/8, 172.16.0.0/12 & 192.168.0.0/16

Following this step is by far the easiest way to ensure, for enterprise licensed customers, all RFC1918 IP ranges can be scanned / reported on going forward.

It also allows for the addition of these RFC 1918 IP ranges into multiple application modules in Qualys, ie, Vulnerability management & Policy compliance.

For a 1 to 1 migration of the current assets being tracked under the host asset menu in Qualys, this python sample code will help achieve this:

**https://github.com/Qualys/API_Driven_Migration/QualysIPProcessor.py**

For a 1 to 1 migration the Host Assets are also re-activated for the Modules they are activated for in the source subscription (VM,PC, CertView, etc.)

When adding the RFC 1918 ranges, you have to ensure you add the host assets to both modules as assets, given that this is tracked, license wise, separately. As with VM host assets, adding the RFC 1918 ranges to the host assets table DOES NOT mean you are actually licensing them, only when the hosts (IP’s) are scanned with a VM/PC scan do we start to track them as the licensed “unique IP‘s scanned” value when oyu have a ENTERPRISE subscription agreement with Qualys.

# Asset Groups

Exporting of asset groups is the next big step post the adding of IP address space to the subscription.

Extracting AG's is done thru the Assets API, starting at page 367, with the AG's being handled on page 423 – 425.

Extract the list of asset groups

/api/2.0/fo/asset/group/?action=list&show_attributes=ALL

This will provide an XML output of all Assetgroups with their contents

- CAUTION –

This will also contain a so called AssetGroup "All" the first Assetgroup ID

This is a system generated AssetGroup and should NOT be added back into the new target subscription

Secondly, the attributes extracted contain the ApplianceID's from the SOURCE subscription.

These will have to be replaced with the applianceID's from the TARGET subscription, which can be obtained thru an API call as well to the /api/2.0/fo/appliance API

Sample Python script for (apart of) this can be found at

**https://github.com/Qualys/API_Driven_Migration** /QualysAssetGroupProcessor.py

## Export user settings (ie, the actual use settings per user)

This is a per user ID call, and will results in a XML per user that needs to be exported.

Documentation starts on page 25 of the API guide and page 618 of the API guide

A call to extract the user_id for all users is this:

https://{{base_url}}/msp/user_list.php

A loop will need to be made to extract all data from the platform.

First make a call to obtain all user_id values from the source subscription.

curl -u "username:password" -H "X-Requested-With:curl" "https://qualysapi.qualys.com/api/2.0/fo/user_prefs/?action=export &user_id=1020428" > export_user_prefs.xml

## Import User settings

curl -u "username:password" -H "Content-type: text/xml" -X "POST" --data-binary @export_user_prefs.xml "https://qualysapi.qualys.com/api/2.0/fo/user_prefs/?action=import &user_id=1022024" > import_user_prefs.xml

Python API script sample:

To perform this automated, please refer to the python code on:

**https://github.com/Qualys/API_Driven_Migration**/QualsyUserProcessor.py

## Subscription level settings

Based on the guidance provided in this (https://www.qualys.com/docs/qualys-subscription-api-user-guide.pdf ) API documentation a large number of settings and configurations can be transferred by means of export / import actions.

An export can be made in a single large call (https://{{base_url}}/api/2.0/fo/subscription/?action=export)
Or in sections should you so want.

We advise to make a single large export of the subscription data as this is required to ensure a as complete as possible transfer to the new environment.

The following settings will be transferred.

- RECORD > SUBSCRIPTION > FO > SCAN > SCANNER_TRUSTED_CA
- RECORD > SUBSCRIPTION > FO > SCAN > EXCLUDED_IPS
- RECORD > SUBSCRIPTION > FO > SCAN > EXCLUDED_IPS_EXPIRATION
- RECORD > SUBSCRIPTION > FO > SCAN > EXCLUDED_HISTORY
- RECORD > SUBSCRIPTION > FO > REPORTS > BUSINESS_RISK
- RECORD > SUBSCRIPTION > FO > REPORTS > BUSINESS_RISK_MATRIX
- RECORD > SUBSCRIPTION > FO > REMEDIATION > SETUP
- RECORD > SUBSCRIPTION > FO > USERS > Setup
- RECORD > SUBSCRIPTION > FO > USERS > SUB_IPV6_RESTRICT_MAP
- RECORD > SUBSCRIPTION > FO > USERS > SUBSCRIPTION_IP_RESTRICT_MAP
- RECORD > SUBSCRIPTION > FO > USERS > IP_RANGE

## How to execute?

The 2 API commands (export & import) are rather straightforward.

Exporting is done this way using CURL:

curl -u "username:password" -H "X-Requested-With:curl" "https://qualysapi.<NDA01 domain name>/api/2.0/fo/subscription/?action=export" > export_config.xml

Import is done this way using CURL

curl -u "username:password" -H "Content-type: text/xml" -X "POST" --data-binary @export_config.xml
"https://qualysapi.qg2.apps.qualys.eu/api/2.0/fo/subscription/?action=import" > import_config.xml

# Transferable settings Policy Compliance

## Export of policies

Since Policy compliance shares a lot of settings (such as user settings) with the Vulnerability Management module, our recommendation is to only export / import the policies.

There are 2 ways to extract the policy information from the platform.

1) Thru the WebUI (select a policy, and on the quick actions menu choose export).
    a. This is the preferred way for a environment with a low number of Policies.
2) Thru the API, which allows for automated export.
    a. Extract list of policy ID's first from platform with this call:
        i. https://{{base_url}}/api/2.0/fo/compliance/policy?action=list
    b. Filter the ID from the XML data, and use the ID's as input for the subsequent calls using this API call:
        i. https://{{base_url}}/api/2.0/fo/compliance/policy?action=export&id=<ID FROM Previous call> &show_user_controls=1&show_appendix=1 > <policyID.xml>

each call will result in an XML file that is needed to import the policy in the target subscription.

## Import of policies

To import policies from the previously exported data, we simply need to reverse the operations from the previous section.

This means that from the UI, the import policy option is selected one a one by one bases.

For the API route, it means the following calls need to be repeated until all policies are imported.

curl -H "X-Requested-With: Curl Sample" -H "Content-type: text/xml" --data-binary @<file with Policy ID.xml -u "USERNAME:PASSWORD" https://{{base_url}}/api/2.0/fo/compliance/policy /?action=import&title=My+Policy

this call needs to be ran in a loop until all policy export files are processed.

UDC's that are exported and imported as part of this process are automatically re-created in the new subscription, assuming this option is selected during export / import.

Any reference to the UDC in the policies is changed should the UDC ID change between platforms.

# Report templates

## Vulnerability management

For the VM application, report templates can be, and thus should be, exported to ensure the same report contents is added to the reports generated in the new environment.

## Export of VM templates

To export the template(s) use the API for the SCAN, MAP, Patch (and if needed PCI) templates

/api/2.0/fo/report/template/scan/?action=export

/api/2.0/fo/report/template/patch/?action=export

/api/2.0/fo/report/template/map/?action=export

/api/2.0/fo/report/template/pciscan/?action=export

## Import of VM templates

/api/2.0/fo/report/template/scan/?action=create

/api/2.0/fo/report/template/map/?action=create

/api/2.0/fo/report/template/patch/?action=create

Each of these calls need to be accompanied with operators that our outlined in the API documentation.

## PCI Merchant Accounts

If your existing subscription is linked to the PCI Merchant portal, please follow the steps below to reestablish the links to your PCI Merchant accounts. Please note: each individual with an VM account and PCI account will need to reestablish the links to the merchant accounts.

1) Thru the WebUI in VM, select Scans > Setup > PCI Account links.
2) Select PCI Account Links.
3) Select Add Existing PCI Account.
4) Provide the credentials the PCI merchant account to link.
5) Thru the API, which allows for automated export.
6) Repeat steps 3 – 5 until all of the required merchant accounts are linked.

## Policy Compliance

At the time of writing this guide, the ability to export/import compliance report templates is not available via API or in the platform UI.

## Policy compliance Scans

Option profiles

Extract the PC option profiles thru this API call:

/api/2.0/fo/subscription/option_profile/pc/?action=list

Creating the option profiles is done thru this API call:

/api/2.0/fo/subscription/option_profile/pc/?action=create

Scan schedules

To list the scan schedules, extract the schedules via this API

api/2.0/fo/schedule/scan/compliance/?active=1&action=list

this will call the ACTIVE scheduled PC scans and provide XML output to be used in the re-creation of the scan schedules using the below API.

/api/2.0/fo/schedule/scan/compliance/?action=create

Code samples from the VM process can be re-used for this using the PC API due to the relative comparability of these.

## API samples

A collection of sample code to use for with the API is available at the following BitBucket location.

https://github.com/Qualys/API_Driven_Migration/

this collection of code is provided – AS IS – with no technical support via the official support organization in Qualys on the code itself. Naturally, API related issues fall under the remit of tech support, and can be raised there like normal.