



# FORESCOUT®

## **Forescout Palo Alto GlobalProtect & IP Stack Integration**

05.16.19 - v1.0

---

Nick Duda

[nduda78@gmail.com](mailto:nduda78@gmail.com)

Twitter: [@nduda78](https://twitter.com/nduda78)

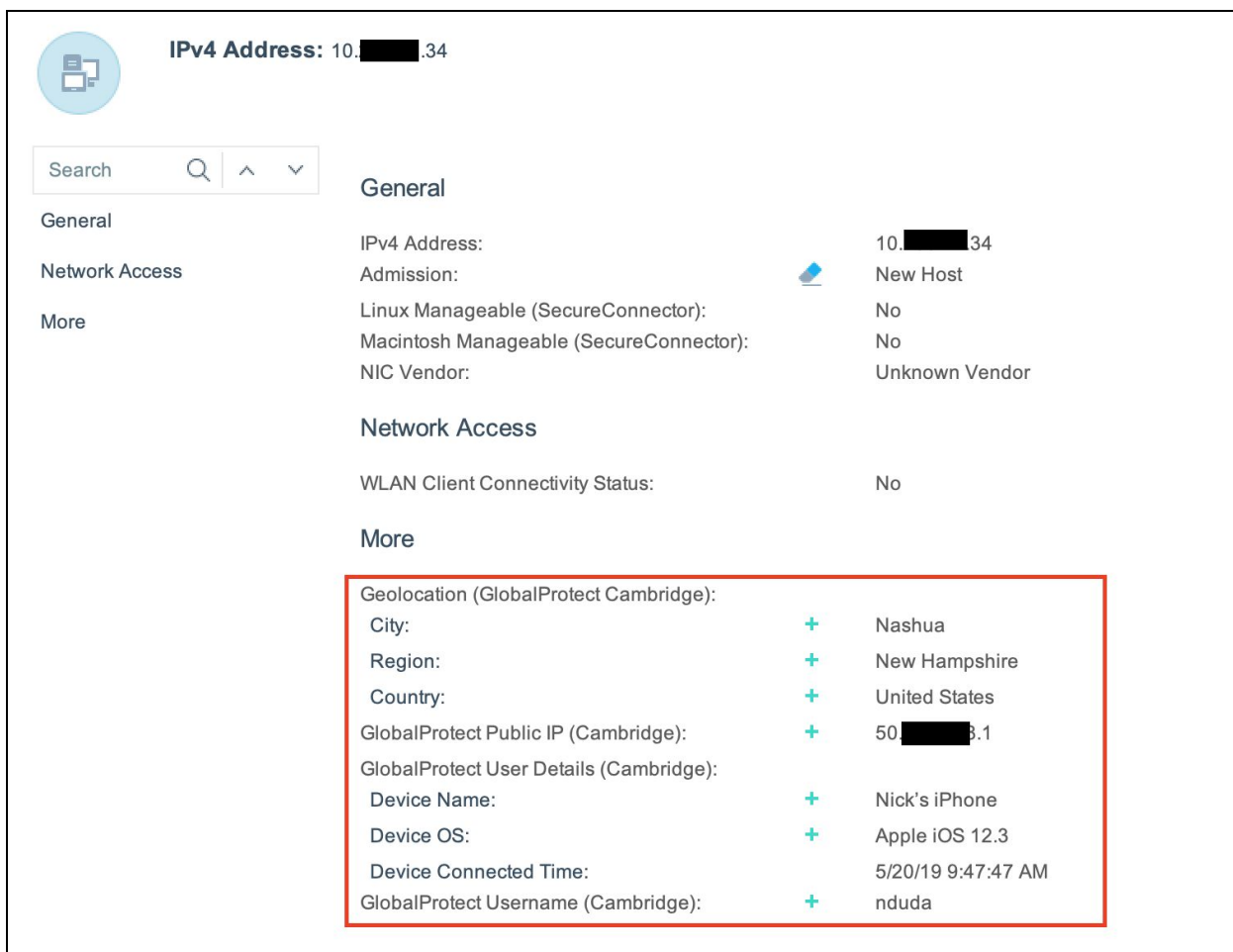
LinkedIn: <https://www.linkedin.com/in/nickduda/>

## Summary

Using the Forescout Open Integrations Module (OIM), this document will walk you through integrating Forescout with Palo Alto GlobalProtect running on PAN-OS (REST API) and IP Stack (ipstack.com). With this integration you will gain the following:

1. Extract GlobalProtect (VPN) connected device information such as:
  - a. User connected
  - b. Device Operating System
  - c. Device Name
  - d. Time the User established connection to the GlobalProtect Gateway
  - e. Connecting device Public IP Address
2. Disconnect users from the GlobalProtect Gateway.
3. Extract Geo Location data from IP Stack using the Public IP Address of the connecting GlobalProtect device.
  - a. City, Zip Code, Region, Country, Continent
  - b. Longitude, Latitude
  - c. Timezone

With the data from these integrations you will gain deeper visibility into remotely connected devices over the GlobalProtect VPN. This information can be used in policies (conditions) as well as {tags}.



The screenshot displays the 'Profile Tab' in the ForeScout interface. At the top, it shows the IPv4 Address as 10.██████.34. Below this is a search bar and a sidebar with tabs for 'General', 'Network Access', and 'More'. The 'General' tab is active, showing fields for IPv4 Address, Admission (with a blue icon), Linux Manageable (SecureConnector), Macintosh Manageable (SecureConnector), and NIC Vendor. The 'Network Access' tab shows WLAN Client Connectivity Status. The 'More' tab is expanded, revealing a red-bordered box containing GlobalProtect data: Geolocation (GlobalProtect Cambridge) with City (Nashua), Region (New Hampshire), and Country (United States); GlobalProtect Public IP (Cambridge) as 50.██████.1; GlobalProtect User Details (Cambridge) including Device Name (Nick's iPhone), Device OS (Apple iOS 12.3), Device Connected Time (5/20/19 9:47:47 AM), and GlobalProtect Username (Cambridge) as nduda.

*Example of the Profile Tab with GlobalProtect and IP Stack data*

## Requirements

### Forescout Requirements

1. Forescout CounterACT v7.x/8.x
2. Open Integrations Module (OIM - Extended Module)

### Palo Alto GlobalProtect Requirements

1. Palo Alto Firewall (GlobalProtect Gateway).
  - a. This has been tested on PAN-OS v8.1.x
2. User account with read-write/permissions to the REST API
  - a. <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api.html>

- b. Read permissions are used to extract GlobalProtect information
- c. Write permissions are used to execute the *request* api endpoint to disconnect users from the VPN.

### IP Stack Requirements

1. Valid API KEY from [www.ipstack.com](http://www.ipstack.com)
  - a. Free Account allows 10,000 requests / month

## Configuration

### Extract Username from GlobalProtect Client IP Address

1. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
2. Add new request
3. General Tab
  - a. Request Name: GlobalProtect IP Address Lookup
  - b. Description: This query will lookup the username associated with IP Address
  - c. HTTP Method: Get
  - d. URL:
 

```
https://<IP_OF_NGFW>/api/?type=op&cmd=<show><user><ip-user-mapping><ip><ip></ip></ip-user-mapping></user></show>
```
4. Authentication Tab
  - a. Use Basic Authentication Header - Provide username and password created for accessing the NGFW REST API
5. CounterACT Devices Tab
  - a. Use Connecting CounterACT Device - Specific a CounterACT appliance that should make these queries.

Edit External Web Service Request

## Edit External Web Service Request

General Authentication CounterACT Devices Traffic Thresholds

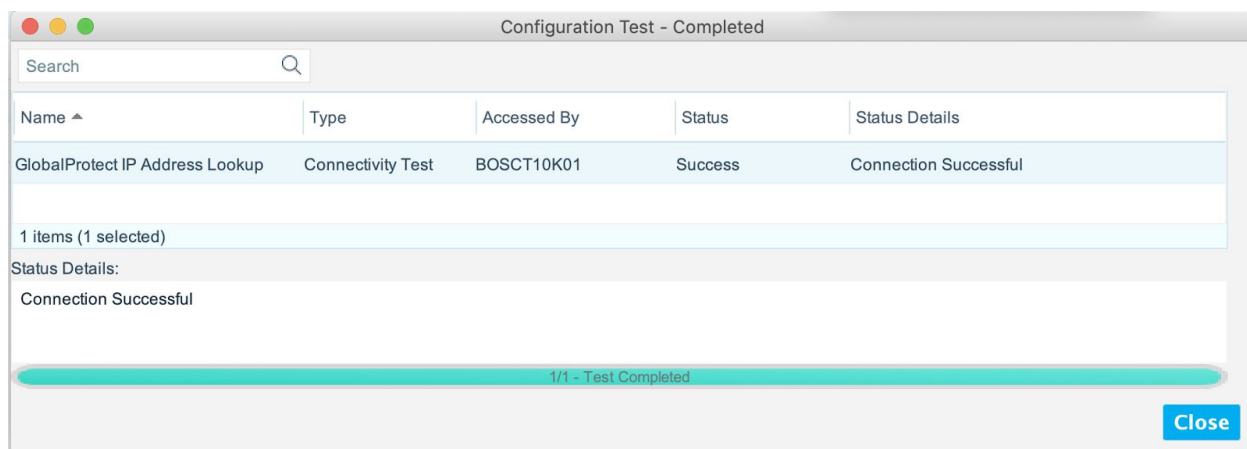
### General

Define an HTTP request message that retrieves data from an external web service. To include endpoint-specific or user-specific information in the request, select Add Tags to insert runtime variables in the URL.

Request Name	GlobalProtect IP Address Lookup
Description	This query will lookup the username associated with IP Address
HTTP Method	GET
URL (with request parameters)	oping><ip>{ip}</ip></ip-user-mapping></user></show>
HTTP Message Headers	
HTTP Request Body	
No Record returns HTTP Status	200

Help OK Cancel

Click OK. After Applying, test the query. Supply the IP Address of a device connected to the GlobalProtect VPN. The query will result a status of Success if the IP address was found.



The XML results of this API query:

```
<response status="success">
  <result>
    <entry>
      <ip>10.251.251.1</ip>
      <vsys>vsys1</vsys>
      <type>GP</type>
      <user>domain\user</user>
      <idle_timeout>9621</idle_timeout>
      <timeout>9622</timeout>
    </entry>
  </result>
</response>
```

6. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Properties

7. Add new property

8. General Tab

a. Property Name: GlobalProtect Username

b. Property Tag: gp\_username

i. Make note of whatever property tag name you use here as it is used in the Extract VPN Connected device user details based on username section below.

- c. Description: Extract username
  - d. Web Service Request: GlobalProtect IP Address Lookup (Web)
- 9. Map Data Tab
  - a. Single Value Property
  - b. Data Type: String
  - c. Parse Data Using: Regular Expression
  - d. Parsing Pattern: <response status="success"><result>.\*<user>\w\*\(?<user>[^\<]\*\)</user>.\*
- 10. Click OK > Apply

After Applying, test the property. Supply the IP Address of a device connected to the GlobalProtect VPN. The query will result in the username associated with the connected device.

```

*** External Web Service Property Test Start ***
Testing property: GlobalProtect Username (Cambridge), type is Single.
Connected to the web service, the response content is
<response
status="success"><result><entry><ip>[REDACTED].34</ip><vsys>vsys1</vsys><type>GP</type><user>
>[REDACTED]\nduda</user><idle_timeout>10782</idle_timeout><timeout>10784</timeout></entry>
</result></response>
, parsing HTTP response...

Parser type is regex
Resolving property GlobalProtect Username (Cambridge)...

It is a Single property.

*** Test is passed. ***
The Web Service Property value is [nduda]

*** Test Finished ***
  
```

## Extract VPN Connected device user details based on username

1. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
2. Add new request
3. General Tab
  - a. Request Name: GlobalProtect User Details
  - b. Description: This query will lookup the vpn connected device user details associated with username
  - c. HTTP Method: Get

## d. URL:

```
https://<IP_OF_NGFW>/api/?type=op&cmd=<show><global-protect-gateway>
<current-user><user>{dextweb_gp_username}</user></current-user></g
lobal-protect-gateway></show>
```

Replace the {tag} with whatever you named it in Step 8b in the *Extract Username from GlobalProtect Client IP Address* section.

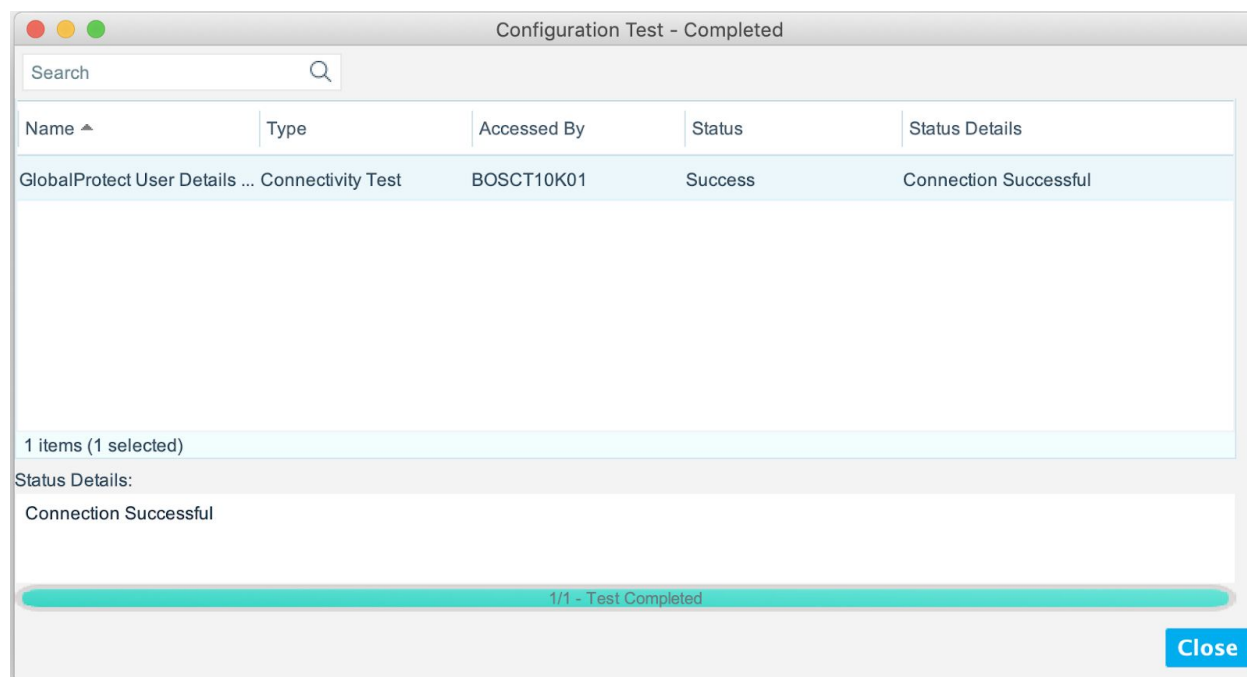
## 4. Authentication Tab

- a. Use Basic Authentication Header - Provide username and password created for accessing the NGFW REST API

## 5. CounterACT Devices Tab

- a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.

Click OK. After Applying, test the query. Supply the username (i.e. nduda) of a user connected to the GlobalProtect VPN. The query will result a status of Success if the username was found.





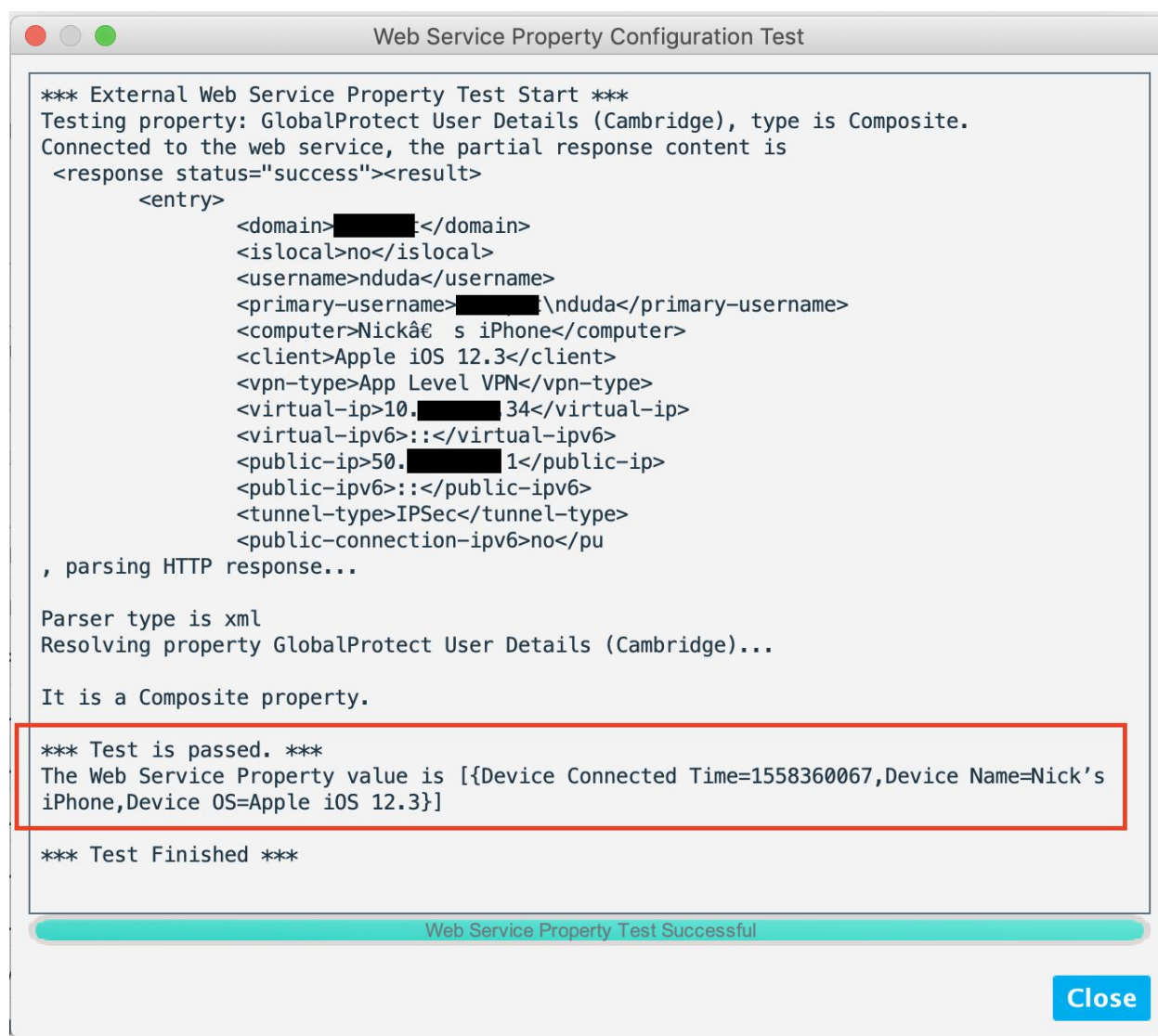
The XML results of this API query:

```
<response status="success">
  <result>
    <entry>
      <domain>acme</domain>
      <islocal>no</islocal>
      <username>nduda</username>
      <primary-username>acme\nduda</primary-username>
      <computer>Nick's iPhone</computer>
      <client>Apple iOS 12.3</client>
      <vpn-type>App Level VPN</vpn-type>
      <virtual-ip>10.x.x.34</virtual-ip>
      <virtual-ipv6>:::</virtual-ipv6>
      <public-ip>50.x.x.1</public-ip>
      <public-ipv6>:::</public-ipv6>
      <tunnel-type>IPSec</tunnel-type>
      <public-connection-ipv6>no</public-connection-ipv6>
      <login-time>May.20 13:47:47</login-time>
      <login-time-utc>1558360067</login-time-utc>
      <lifetime>2592000</lifetime>
    </entry>
  </result>
</response>
```

6. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Properties
7. Add new property
8. General Tab
  - a. Property Name: GlobalProtect User Details
  - b. Property Tag: **gp\_userdetails**
  - c. Description: Extract device user details
  - d. Web Service Request: GlobalProtect User Details (Web)
9. Map Data Tab

- a. Composite Property
    - i. Parsing Data Using: XML Path
    - ii. Add the follow three properties
  - b. Name: Device Name
    - i. Parsing pattern: /response  
[@status='success']/result/entry/computer/text()
    - ii. Date Type: String
  - c. Name: Device OS
    - i. Parsing Pattern: /response  
[@status='success']/result/entry/client/text()
    - ii. Data Type: String
  - d. Name: Device Connected Time:
    - i. Parsing Pattern: /response  
[@status='success']/result/entry/login-time-utc/text()
    - ii. Data Type: Date
    - iii. Epoch Time
10. Click OK > Apply

After Applying, test the property. Supply the username (i.e. nduda) of a user connected to the GlobalProtect VPN. The query will result a status of Success if the username was found.



## Obtain connected device public IP address to be used for IP Stack

We have to create another web service property that is a list value because composite properties don't have associated tags for each property. If you don't plan on using IP Stack (or another geolocation service) then you can skip these IP Stack sections.

1. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Properties
2. Add new property
3. General Tab
  - a. Property Name: GlobalProtect Device Public IP Address
  - b. Property Tag: gp\_device\_public\_ip

- i. Make note of whatever property tag name you use here as it is used in the Obtain Geolocation data based on the public IP address of the connected device section below.
  - c. Description: Extract device public IP address
  - d. Web Service Request: GlobalProtect User Details (Web)
4. Map Data Tab
  - a. Single Value Property
  - b. Data Type: String
  - c. Parse Data Using: XML Path
  - d. Parsing Pattern: /response [@status='success']/result/entry/public-ip/text()
5. Click OK > Apply

Test the property and the results should just be the public IP address.

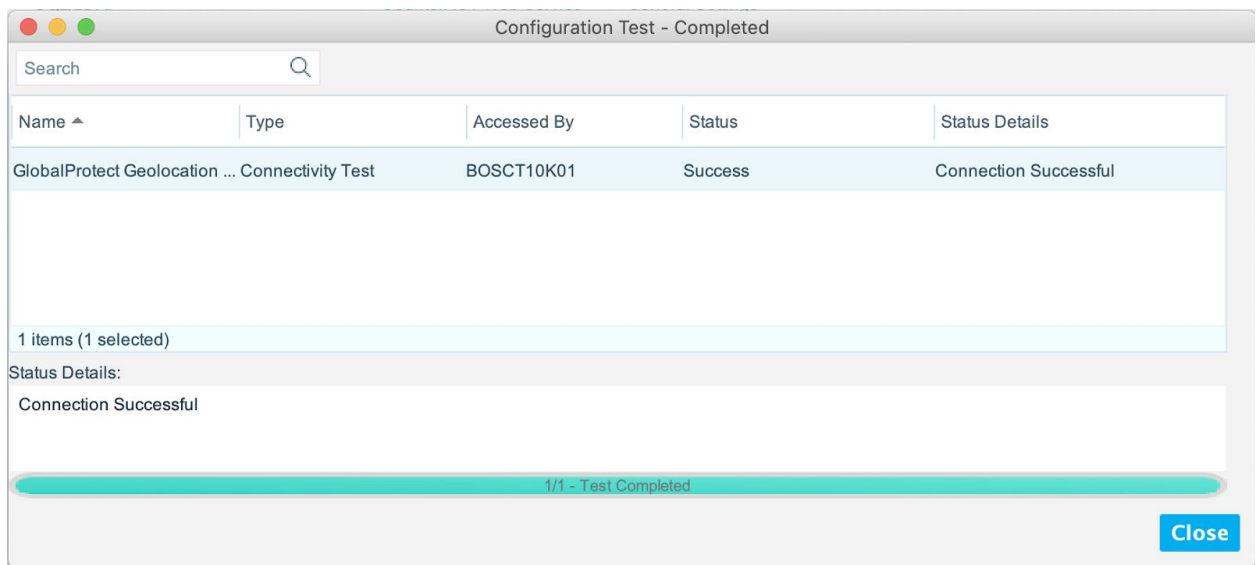


## Obtain Geolocation data based on the public IP address of the connected device.

1. Create an account at [www.ipstack.com](http://www.ipstack.com)
  - a. Free account allows 10,000 requests / month
  - b. Once an account is created, obtain the API key from your dashboard.
2. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Web Service Request
3. Add new request
4. General Tab
  - a. Request Name: GlobalProtect Geolocation
  - b. Description: This query will lookup the geolocation associated with the connected IP Address
  - c. HTTP Method: Get
  - d. URL:  
`http://api.ipstack.com/{dexextweb_gp_device_public_ip}?access_key=INSERT_YOUR_API_KEY&format=1`

5. Authentication Tab
  - a. No Authentication since the API key is in the request URL
6. CounterACT Devices Tab
  - a. Use Connecting CountetACT Device - Specific a CounterACT appliance that should make these queries.
7. Click OK > Apply

Test the web request:



8. Forescout Console > Options > Data Exchange (DEX) > External Web Services > Properties
9. Add new property
10. General Tab
  - a. Property Name: GlobalProtect Device Geolocation
  - b. Property Tag: **globalprotect\_ip\_stack\_data**
  - c. Description: Extract Geolocation data from IP Stack
  - d. Web Service Request: GlobalProtect Geolocation (Web)
11. Map Data Tab
  - a. Composite Property
    - i. Parsing Data Using: JSON Path
    - ii. Add the follow three properties
  - b. Name: City
    - i. Parsing pattern: \$.city
    - ii. Date Type: String
  - c. Name: Region
    - i. Parsing Pattern: \$.region\_name

- ii. Data Type: String
- d. Name: Country
  - i. Parsing Pattern: \$.country\_name
  - ii. Date Type: String

12. Click OK > Apply

Test the property by supplying the Public IP address of a device connected to the VPN. There are a bunch more data IP Stack gives you, just add them into the composite property if you want to use them.



```

*** External Web Service Property Test Start ***
Testing property: Geolocation (GlobalProtect Cambridge), type is Composite.
Connected to the web service, the partial response content is
{
  "ip":"50.██████.1",
  "type":"ipv4",
  "continent_code":"NA",
  "continent_name":"North America",
  "country_code":"US",
  "country_name":"United States",
  "region_code":"NH",
  "region_name":"New Hampshire",
  "city":"Nashua",
  "zip":"03062",
  "latitude":42.724,
  "longitude":-71.479,
  "location":{
    "geoname_id":5090046,
    "capital":"Washington D.C.",
    "languages":[
      {
        "code":"en",
        "name":"English",
        "native":"English"
      }
    ]
  },
  "country_fl
, parsing HTTP response...

Parser type is json
Resolving property Geolocation (GlobalProtect Cambridge)...

It is a Composite property.

*** Test is passed. ***
The Web Service Property value is [{City=Nashua,Country=United States,Region=New
Hampshire}]

*** Test Finished ***
  
```

Web Service Property Test Successful

## JSON Results from IP Stack

```
{
  "ip": "144.x.x.106",
  "type": "ipv4",
  "continent_code": "NA",
  "continent_name": "North America",
  "country_code": "US",
  "country_name": "United States",
  "region_code": "NH",
  "region_name": "New Hampshire",
  "city": "Portsmouth",
  "zip": "03801",
  "latitude": 43.0729,
  "longitude": -70.8052,
  "location": {
    "geoname_id": 5091383,
    "capital": "Washington D.C.",
    "languages": [
      {
        "code": "en",
        "name": "English",
        "native": "English"
      }
    ]
  },
  "country_flag": "http://assets.ipstack.com/flags/us.svg",
  "country_flag_emoji": "\ud83c\uddfa\ud83c\uddf8",
  "country_flag_emoji_unicode": "U+1F1FA U+1F1F8",
  "calling_code": "1",
}
```

```
"is_eu":false  
}  
}
```

## Using all this data

1. I would recommend updating your Options > Discovery.
  - a. Create a new discovery rule, apply it to your VPN segments and discover the new Properties you created in this document. This way as new devices connect all the GlobalProtect and IP Stack data will be obtained so you can use it in policy. This will also display all the data on the profile tab.
  - b. NOTE: Keep tabs on your IP Stack requests. If using the free account 10,000 requests a month might go quickly.
2. Use these properties in policies. These properties can help with:
  - a. Figuring out remote, company assets connecting
  - b. Integrating with further technology, such as MDM solutions
  - c. Controlling access of devices connecting from locations not approved.
  - d. Overall visibility.

## Disconnecting a device from the GlobalProtect VPN

1. In Progress





IPv4 Address: 10.██████.34

## General

## Network Access

## More

## General

IPv4 Address:

Admission:

Linux Manageable (SecureConnector):

Macintosh Manageable (SecureConnector):

NIC Vendor:

10.██████.34

New Host

No

No

Unknown Vendor

## Network Access

WLAN Client Connectivity Status:

No

## More

Geolocation (GlobalProtect Cambridge):

City:



Nashua

Region:



New Hampshire

Country:



United States

GlobalProtect Public IP (Cambridge):



50.██████.1

GlobalProtect User Details (Cambridge):

Device Name:



Nick's iPhone

Device OS:



Apple iOS 12.3

Device Connected Time:

5/20/19 9:47:47 AM

GlobalProtect Username (Cambridge):



nduda