

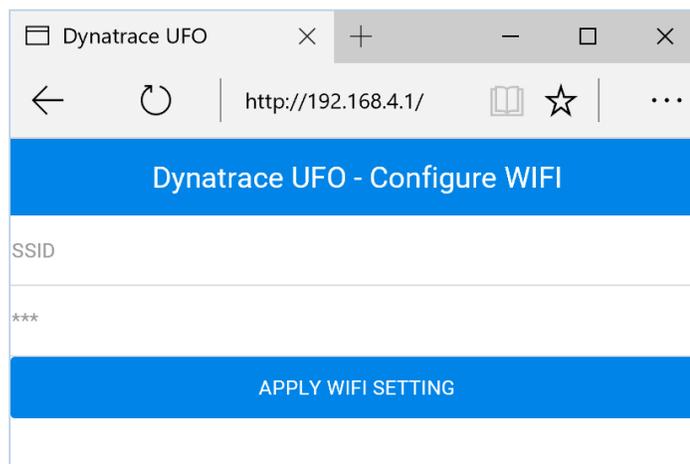
Setting up Dynatrace UFO in a Managed Environment via DMZ Activegate

Prerequisites:

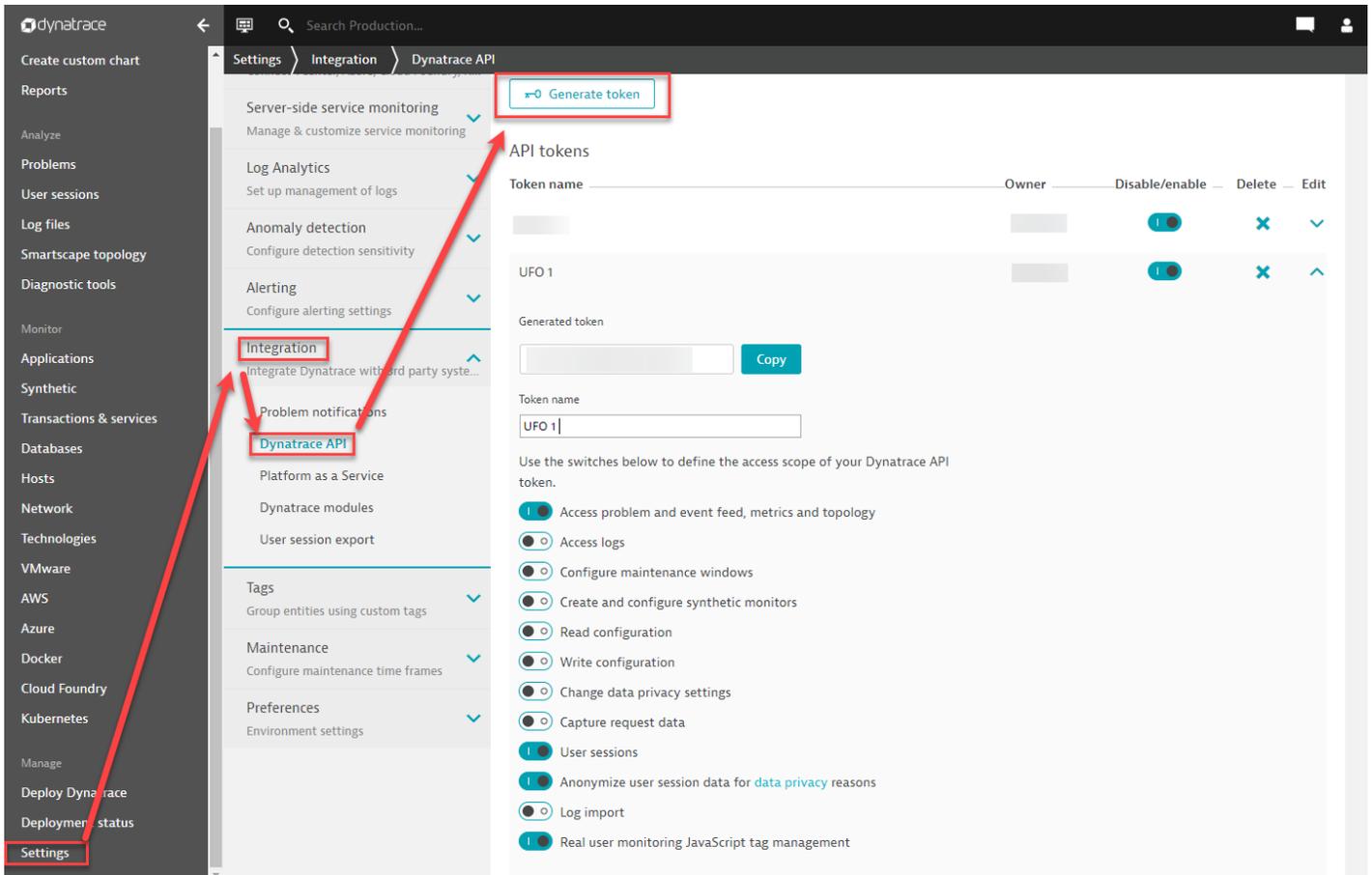
UFO – Dynatrace Managed Admin Permissions – ActiveGate – Wifi Access

Most of this information can be found at: <https://github.com/Dynatrace/ufo/tree/master/quickstart>

1. Connect your UFO to a power supply – 2,000mA USB Charger
2. Press the reset button on the UFO. As default and when pressing the hardware reset button at the top of the UFO, the UFO starts a WiFi access point with an SSID named "ufo". (if you cannot see the "ufo" SSID, click the wiFi reset button) - the UFO alternates a single blue ring.
3. Connect a Web browser enabled device (laptop, tablet, smartphone) to the UFO's Wifi with the SSID "ufo" and navigate to <http://192.168.4.1> - Once connected the UFO blinks with a second blue ring
4. Configure UFO WiFi settings so that the UFO connects to your WiFi (Note: WPA2 works well, but enterprise WPA2 and PEAP authentication is not yet available) - whenever the UFO is trying to connect to your WiFi, the UFO blinks yellow. So you can declare connection success when the yellow stops blinking.

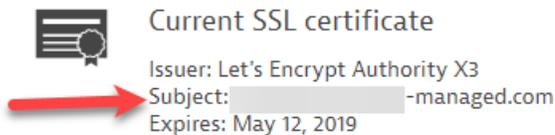


5. Once Connected, It would be wise to ensure that the UFO has the most current firmware by selecting 'Firmware Update' .
6. Navigate to the Firmware section within the UI and update the firmware to the most current. Once updated the UFO will restart and may get a new IP Address.
7. Navigate to your Dynatrace Managed Instance and sign in as an administrator as you will need access to the settings tab. Navigate to your environment you'd like the ufo to connect to. Select 'Settings' → 'Integration' → 'Dynatrace API' → 'Generate Token' From there you will provide the token a meaningful name, as well as access scopes for the token.



- Keep that screen handy as we will need to come back and copy that token. Lets navigate to the Dynatrace Activegate via the Dynatrace CMC and gather the public address so the UFO can pass through it. An Activegate is needed if you cannot access your Dynatrace UI on the same WiFi signal that the UFO is on. Copy that subject string and toss it into a text file and include the port number the OneAgent use as it will be needed later.

Cluster ActiveGate SSL certificate



- Navigate back to your environment dashboard and Copy your Environment ID. This can be found after `.dynatrace-managed.com/` and toss it into that test file.
Your String should look like this now: `https://{active gate url}://{Port}/e/{TENANT ID}`
- Navigate back to your UFO UI and Select 'Dynatrace Integration' and supply the following



Connect your UFO to a Dynatrace Server to query the problem API.
Following metrics will then be visualized by the UFO:

open Application problems

open Infrastructure problems

open Service problems

Enabled **Dont, forget to check the box to enable this**



Paste the string we just made here

Paste the Token Code here

10 **← Refresh rate in seconds**

11. If you have no open issues then the UFO should turn green once it is connected.



12. That's it! You are now fully connected!

Connect your UFO to a Dynatrace Server to query the problem API.
Following metrics will then be visualized by the UFO:

- Open application problems (red)
- Open service problems (purple)
- Open infrastructure problems (yellow)

Only the three most severe problems will be shows.