

# RTCaas Middleware Installation and Configuration

## Introduction

The RTCaaS Middleware translates secure authenticated REST API calls from external components such as the SecureX Orchestrator to calls against ISE over pxGrid or the Active Directory over LDAP.

- Broker between SecureX RTC and ISE (and AD)
- REST API
  - rtc GetUserByIP. (retrieves username and MAC from IP from Cisco ISE)
  - rtcGetUserInfo (retrieves user info from AD: userPrincipalName, AD groups, Lastlogon...)
  - rtcANCApply



Figure 1 RTCaaS Middleware - Overview

Currently the following calls are available

- Retrieve username and MAC address from IP address
- Retrieve information about user such as group membership, last login etc from the Active Directory, given a username
- Apply or clear ISE ANC policy for an endpoint given IP or MAC

### 1. Run docker-compose up

On a machine with docker and docker-compose installed, download the docker-compose.yml file and run docker compose.

```
ubuntu@ip-100-125-2-91:~/RTC$ ls
docker-compose.yml
ubuntu@ip-100-125-2-91:~/RTC$ docker-compose up
Creating network "rtc_my-net" with driver "bridge"
Pulling db (mongo:)... 
latest: Pulling from library/mongo
```

Figure 2 Installation with docker-compose

## 2. Login to RTCaaS Middleware Web GUI

Login to the middleware by browsing to <https://<your ip address>>. You will have to accept certificate warning.

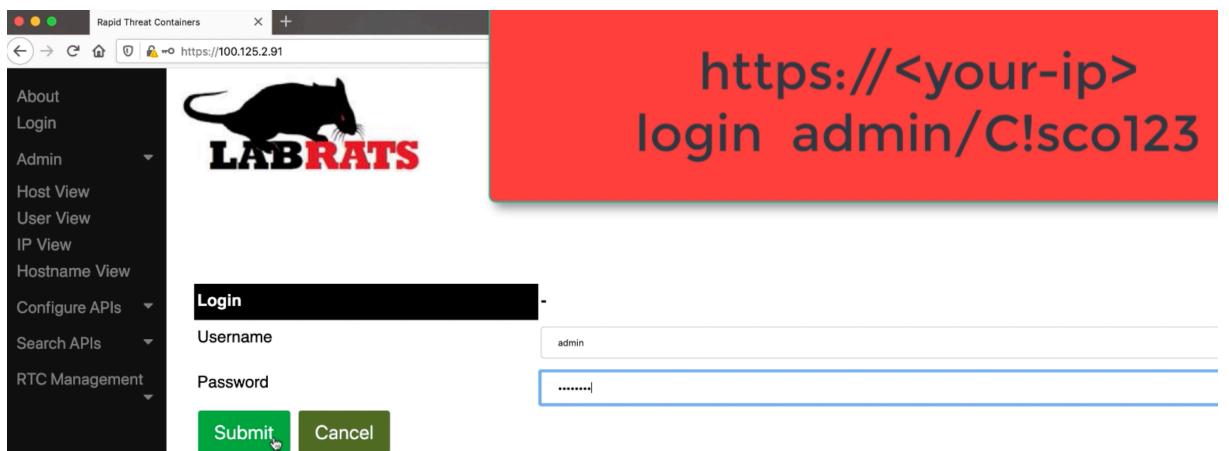


Figure 3 Logging in to the Web UI

Username admin.

Password C!sco123.

## 3. Hardening: Configure Trusted Networks.

By default, all IP addresses can connect to the middleware. Change this by

- Add a trusted network for your admins (e.g. bastion hosts)
- Add a trusted network for your SXO
- Delete the default network

You can find out the public IP of the SXO by creating a trivial workflow that connects to a REST API such as [ipify.com](http://ipify.com)

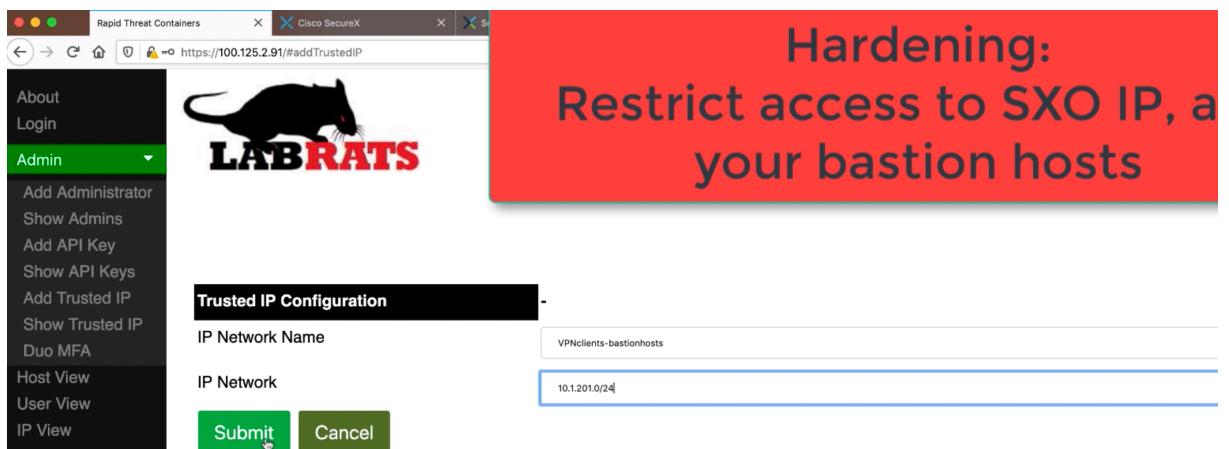


Figure 4 Adding a Trusted IP

The screenshot shows a web browser window with three tabs: 'Rapid Threat Containers', 'Cisco SecureX', and 'SecureX Orchestrator: Workflow'. The main content area features a black rat logo and the text 'LABRATS'. A sidebar on the left is titled 'Admin' and includes options like 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', 'Duo MFA', 'Host View', and 'User View'. The central part of the page displays a table titled 'Trusted Networks' with two entries:

Name	IP Network	Delete
SXO	35.174.245.8	[Delete]
VPNclients-bastionhosts	10.1.201.0/24	[Delete]

Figure 5 After adding trusted IPs and deleting default

#### 4. Hardening: Add New Admin User and default admin

Add a new admin user with a password.

The screenshot shows a web browser window with three tabs: 'Rapid Threat Containers', 'Cisco SecureX', and 'SecureX Orchestrator: Workflow'. The main content area features a black rat logo and the text 'LABRATS'. A sidebar on the left is titled 'Admin' and includes options like 'Add Administrator', 'Show Admins', 'Add API Key', 'Show API Keys', 'Add Trusted IP', 'Show Trusted IP', 'Duo MFA', 'Host View', 'User View', 'IP View', 'Hostname View', and 'Configure APIs'. A large red callout box on the right contains the text: 'Hardening: Create new user and delete default admin'. The central part of the page displays a form titled 'Administrator Configuration' with fields for 'Username' (set to 'hacke'), 'Password' (redacted), and 'Role' (set to 'Admin'). There are 'Submit' and 'Cancel' buttons at the bottom.

Figure 6 Adding a new admin user

Delete the old admin user (admin).

*It is advisable to first logout and test login as the newly created user, before deleting admin account. If you want to apply Duo MFA as in step 5, it is best to wait until after Duo MFA has been implemented and tested before deleting the admin user.*

## 5. Hardening: Configure Duo Protect to enable MFA for users.

The middleware supports MFA with Duo.

Enter the duo host, I-KEY and S-KEY (from the Duo Portal configuration).

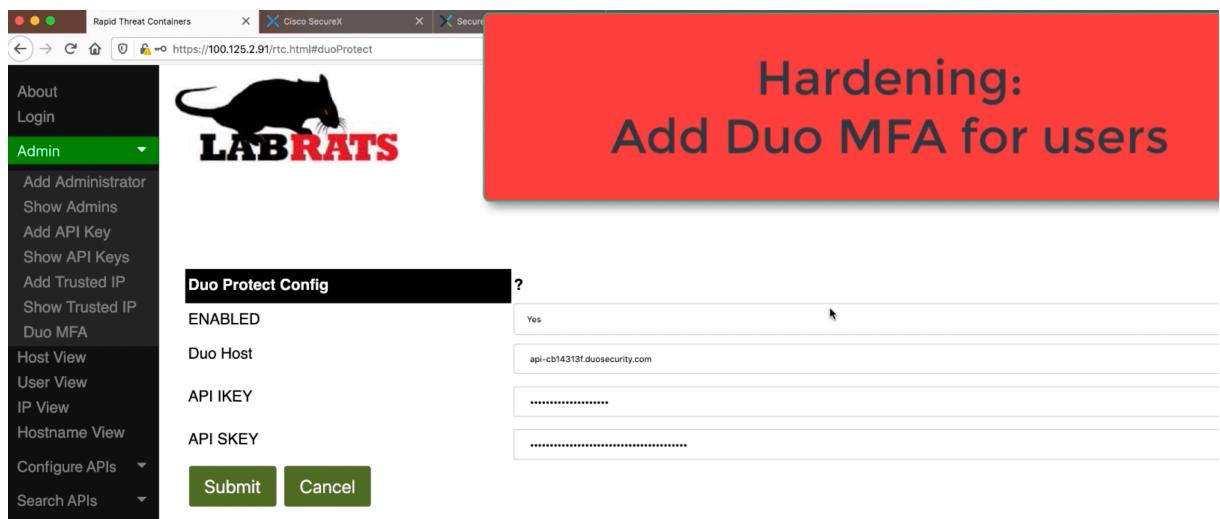


Figure 7 Duo Protect Configuration

After configuring Duo Protect, all users will require to use MFA except any user called "admin". You can test by logging out and in again with any username except "admin".

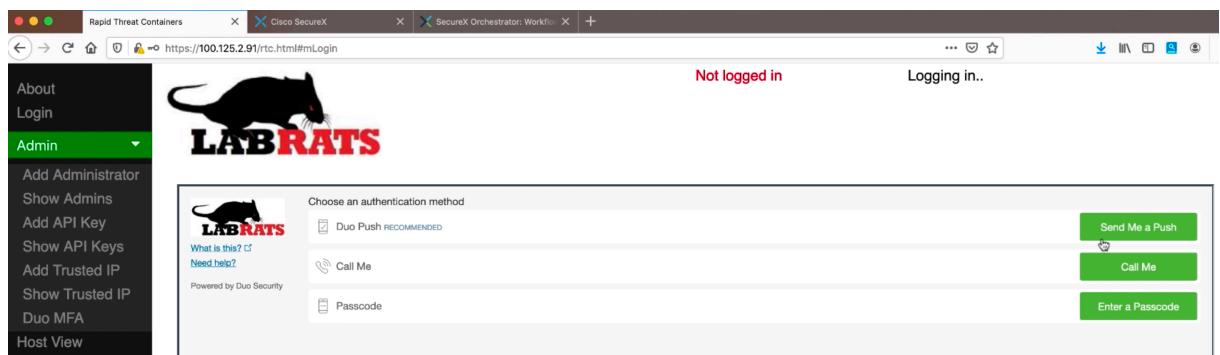


Figure 8 Logging in with Duo MFA

## 6. Configure and Test the Active Directory Interface

Configure the Active Directory interface with

- Server ip
- Base DN
- The username and password of a user that can browse the Active Directory

The screenshot shows a web-based configuration interface for 'Active Directory Configuration'. The left sidebar has a dark theme with white text, listing various configuration options under 'Configure APIs' and 'RTC Management'. The main area has a light background with a red header bar containing the text 'Add Active Directory Config'. Below the header, there are several input fields:

- ENABLED:** A dropdown menu showing 'Yes'.
- AD SERVER:** An input field containing '100.120.120.9'.
- AD BASE DN:** An input field containing 'dc=labrats,dc=se'.
- AD USERNAME:** An input field containing 'hacke@labrats.se'.
- AD PASSWORD:** An input field containing '.....' (redacted).
- SELECT AD GROUPS:** A dropdown menu.

At the bottom are two buttons: 'Submit' and 'Cancel'. A video player control is visible at the very bottom of the page, showing a timeline from 02:59 to -03:58.

Figure 9 Configuring Active Directory

You can test the Active Directory Interface by searching for a user that exists in thee active directory.

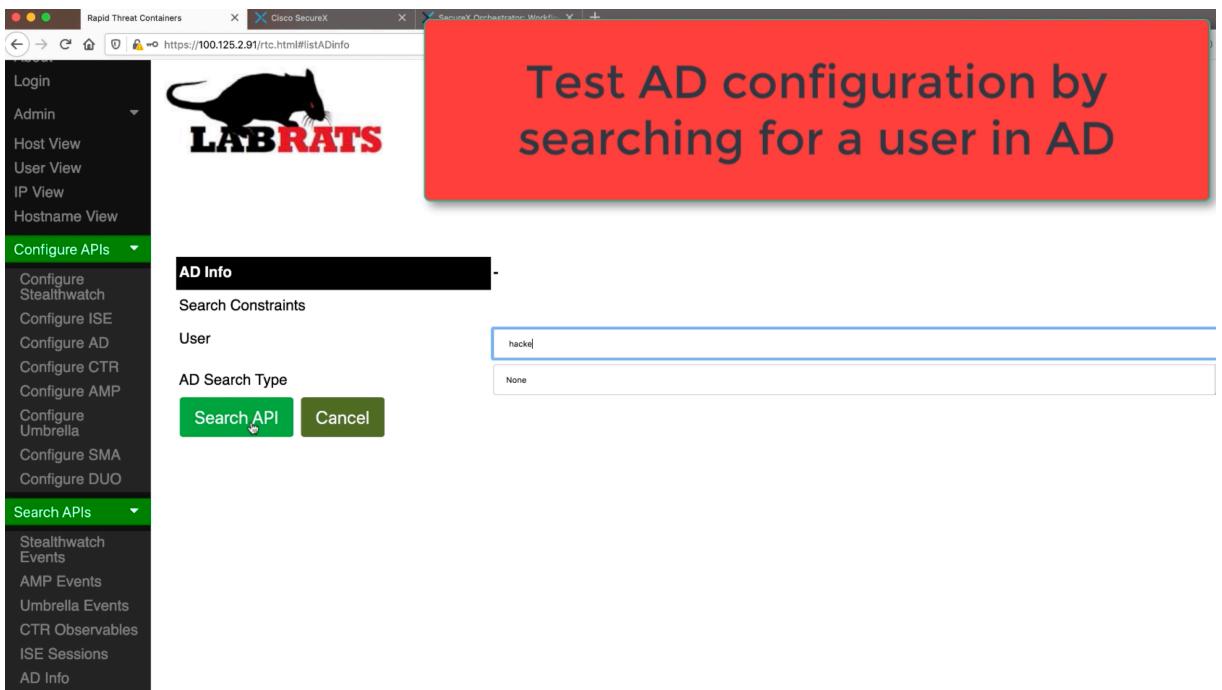


Figure 10 Test AD configuration

The screenshot shows a table titled 'AD Info' displaying user attributes and their values. The columns are 'Attribute Name' and 'Value'. The data is as follows:

Attribute Name	Value
Account Name	hacke
User Principal Name	hacke@labrats.se
Distinguished Name	CN=hacke,OU=Users,OU=Admin,DC=labrats,DC=se
Mail	hacke@labrats.se
MemberOf	CN=HR,OU=Lab,DC=labrats,DC=se
MemberOf	CN=SFDC,OU=Users,OU=Cisco,DC=labrats,DC=se
MemberOf	CN=WSAadmins,OU=Equipment,OU=Admin,DC=labrats,DC=se
MemberOf	CN=Sponsors,OU=Lab,DC=labrats,DC=se

Figure 11 Test AD result (displaying groups and other info)

## 7. Configure and Test the ISE pxGrid Interface

The middleware currently only supports authentication with (dynamically generated) pre-shared key to the pxGrid bus. Manual Approval in the ISE GUI is therefore required.

Prepare by opening a separate tab in your browser and login to ISE, browsing to the page with pxGrid clients (ISE : Administration/pxGrid Services)

In the middleware, configure the ISE API by specifying

- IP address of ISE server
- Username of ERS user (should be ERSadmin in ISE)
- Password of ERS user
- Nodename of pxGrid client, e.g. the middleware (must be unique)

The screenshot shows a web browser window with three tabs: 'Rapid Threat Containers', 'Cisco SecureX', and 'SecureX Orchestrator: Workflow'. The 'Cisco SecureX' tab is active, displaying the URL <https://100.125.2.91/rtc.html#editISE>. The page is titled 'ISE Configuration' and shows the following fields:

Setting	Value
ENABLED	Yes
ISE SERVER	100.120.120.38
ISE USERNAME	ERSadmin
ISE PASSWORD	.....
PXGRID NODE NAME	RTCdemo
PXGRID PASSWORD (SET DYNAMICALLY)	-
PXGRID CLIENT CERT	[Empty Input Field]

The left sidebar menu includes options like Login, Admin, Host View, User View, IP View, Hostname View, Configure APIs (which is selected), Search APIs, and Stealthwatch Events. The 'Configure APIs' section contains sub-options: Configure Stealthwatch, Configure ISE, Configure AD, Configure CTR, Configure AMP, Configure Umbrella, Configure SMA, and Configure DUO. The 'ISE Configuration' form has a 'Logged in as hacke' status and a 'Logout' link.

Figure 12 Configure ISE

After submitting the ISE configuration, you must approve the client in the ISE GUI. This has to be done within 4 minutes from configuring ISE in the middleware.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. In the center, there is a table titled 'All Clients' listing various pxGrid nodes. The columns include Client Name, Description, Capabilities, Status, Client Group(s), Auth Method, and Log. A red box highlights the 'Approve' button in the top right corner of the table header. A large red overlay box with the text 'Approve node in ISE GUI' is overlaid on the bottom right.

Figure 13 Approve pxGrid node in ISE GUI

You can test the ISE pxGrid connection by searching ISE API, which should show all connected sessions if it works. In Middleware GUI, Search APIs -> ISE Sessions.

The screenshot shows a browser window displaying the output of a search API query. The results are titled 'ISE Sessions' and show a table with columns: User Name, MAC, IP, SGT, OS, Profile, NAS, and Port. The table lists several sessions, including CN=mordiac, CN=mephisto, CN=VMRAT31, and CN=garfield. A red box highlights the 'ISE Sessions' section. A large red overlay box with the text 'Verify pxGrid connection with ISE' is overlaid on the bottom right.

Figure 14 Output from Search API / ISE Sessions

User Name	MAC	IP	SGT	OS	Profile	NAS	Port
CN=mordiac,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se	00:0C:29:15:69:FA	10.1.33.13	Employees	Windows 7 Enterprise	Windows7-Workstation	10.1.40.253	GigabitEth
CN=mephisto,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se	00:0C:29:76:99:F8	10.1.33.32	Employees	Windows 7 Professional	Windows7-Workstation	10.1.40.253	GigabitEth
CN=VMRAT31,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se	00:0C:29:CF:3F:15	169.254.87.251	Employees	Windows 10 Enterprise	Windows10-Workstation	10.1.40.253	GigabitEth
CN=garfield,OU=WiredDot1X,OU=Lab,DC=labrats,DC=se	00:50:56:8B:95:4A	10.1.33.33	Employees	Windows 10 Enterprise	Windows10-Workstation	10.1.40.253	GigabitEth

## 8. Generate API key

The API calls are authenticated with an API key. Generate the API key and copy it to notepad or similar.

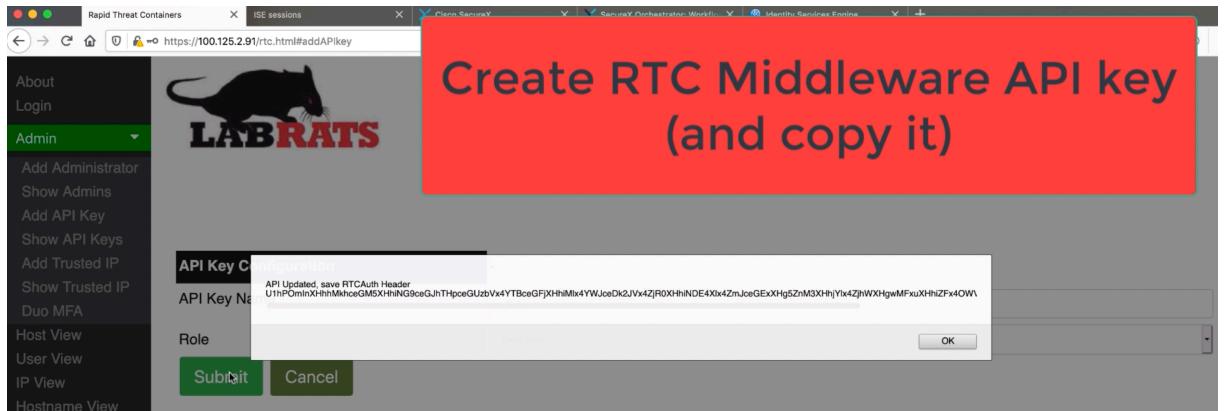


Figure 15 Add API key for SecureX Orchestrator.

The API key has to be present in all calls in a custom header RTCAuthz.

## 9. SXO – Create Secure String Variable with API Key

In SXO, create a Secure String Variable with the API key from previous step.

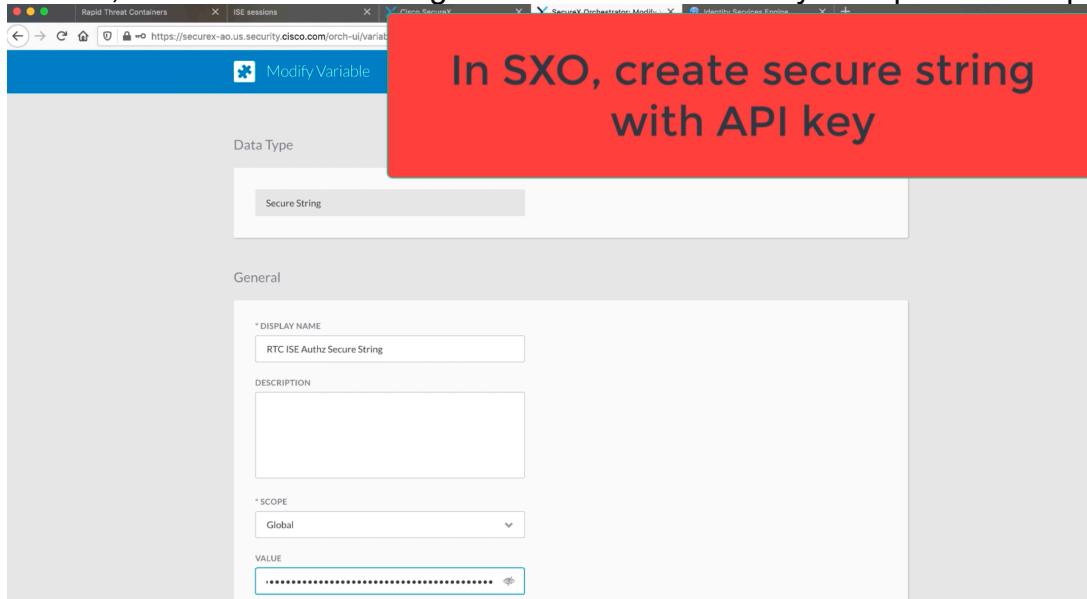


Figure 16 Create Secure String Variable with API key

## 10. SXO – Create Target

In SecureX Orchestration, create a Target that points to your RTC Middleware.

- Protocol HTTPS
- Specify hostname/IP of your Middleware
- Path /cgi-bin
- Check Disable Server Certificate Validation

The screenshot shows a 'Modify Target' interface for an 'HTTP' target. The 'PROTOCOL' dropdown is set to 'HTTPS'. The 'HOST/IPADDRESS' field contains 'rtcaws.labrats.se'. The 'PATH' field contains '/cgi-bin'. A checked checkbox at the bottom left is labeled 'DISABLE SERVER CERTIFICATE VALIDATION'.

Figure 17 SXO - specify target

## 11. SXO - Creating web requests to the RTC Middleware

In SXO when you create a workflow with a web request to the RTC middleware, ensure that

Target is set to the target defined in previous step

Override Workflow Target

\* TARGET

rtcISE

Use Workflow Target Group

Override Workflow Target Group Criteria

You add a custom header named RTCAuthz with the value of the Secure String from previous step.

### CUSTOM HEADERS

HEADER

VALUE

RTCAuthz

\$global.RTC ISE Authz Secure St...

### COOKIE

Ensure that the request relative url and body are set according to the API request.

API call	Relative URL	Method	Body
Get User By IP	/rtcAPIgetUserByIP.py	POST	{"ip": "10.1.33.33"}
Get User Info from Username	/rtcAPIgetUserInfo.py	POST	{"user": "hacke"}
Apply ANC	/rtcAPlancApply.py	POST	{"ip": "10.1.33.33"}
Clear ANC	/rtcAPlancClear.py	POST	{"ip": "10.1.33.33"}