Postman and RESTful API

Task – 1: Open Postman and Configure

**Objective**: Get the Postman tool ready to be used with the R81 Management API. Import the R81 Management API Postman collection.

|  |  |
| --- | --- |
|  | New Versions of Postman require an account. **If** you have an account **or** if you are willing to sign up, follow step 1 to download and install Postman. Otherwise, use the Portable version as described below. |

* To use the latest version of Postman (account is required), from the win\_10 Jump box, open a web browser, and navigate to https://postman.com/downloads/ and download and install the latest postman version.

A screenshot of a computer

Description automatically generated

1. Locate the Postman folder on the desktop and launch the postman-portable application.

A screenshot of a computer

Description automatically generated

1. Navigate to the settings windows in Postman.

A screenshot of a computer

Description automatically generated

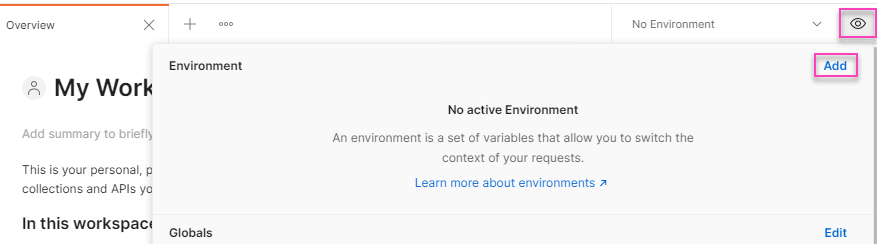
1. Disable the SSL certificate verification.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
|  | *This step is necessary as we have a self-signed certificate on our Gaia servers.* |

1. Next click the eye on the top right and click add.



1. Click Add and use the following to create an environment – Click Add after the values are filled in

* Environment Name: MGMT API
* Server: https://10.0.1.100/web\_api

A screenshot of a computer

Description automatically generated

1. Next click Save and exit out of the Manage Environments window.
2. Select the new Environment MGMT API

A screenshot of a computer

Description automatically generated

1. The API collection files for Postman are provided by R&D. **Download and Extract version 1.9 from the link below (Kudos to Eric Beasley)**.

https://community.checkpoint.com/t5/API-CLI-Discussion/Postman-Collections-links-to-all-available-and-the-basics/td-p/40923

A screenshot of a computer

Description automatically generated

1. Click the import button on the top left of the screen.

A screenshot of a computer

Description automatically generated

1. Click on the Collections tab on the left side of the screen to see the R81.20 Web API calls

A screenshot of a computer

Description automatically generated

Task – 2: Login and do a simple task

**Objective**: Use Postman to do a simple task with the R81.20 Management API

1. Use the filter at the top of the Postman application and type login into the filter area. Alternately, open the first folder in the collection “01 Session Management”.
2. The selections should have changed to only items with login as part of their name.
3. Select login. A new tab is opened on the right for this function call. Click the Body
4. Change the credentials in the body to the following. Make sure you keep the formatting JSON compliant.
   1. "user": "api\_user",
   2. "password": "Cpwins!1",

A screenshot of a computer

Description automatically generated

1. Before we click Send, review the {{server}} in the Post Path. This matches our environment and is how Postman knows how to connect to the R81.20 management server at https://10.0.1.100/web\_api

A screenshot of a computer

Description automatically generated

1. Now click the blue Send button

A screenshot of a computer

Description automatically generated

1. At the bottom of the page, we have the results that were returned from the API server. There are a number of items to look at.
   1. The session ID sid
   2. The status of the request 200

A screenshot of a computer

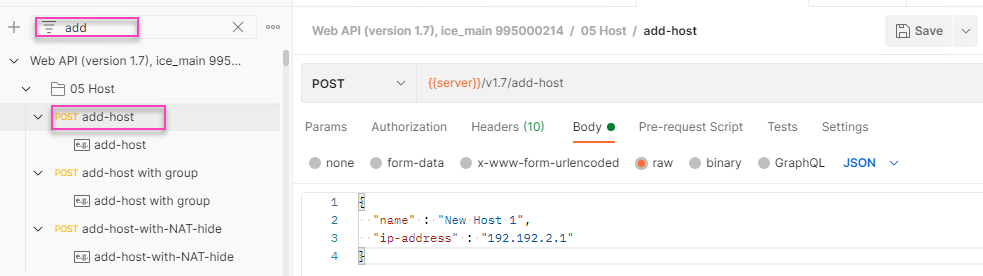
Description automatically generated

1. Postman will automatically add the contents of the sid to the session environment variable we setup earlier. Doing so allows us to run another command and reuse the same session.

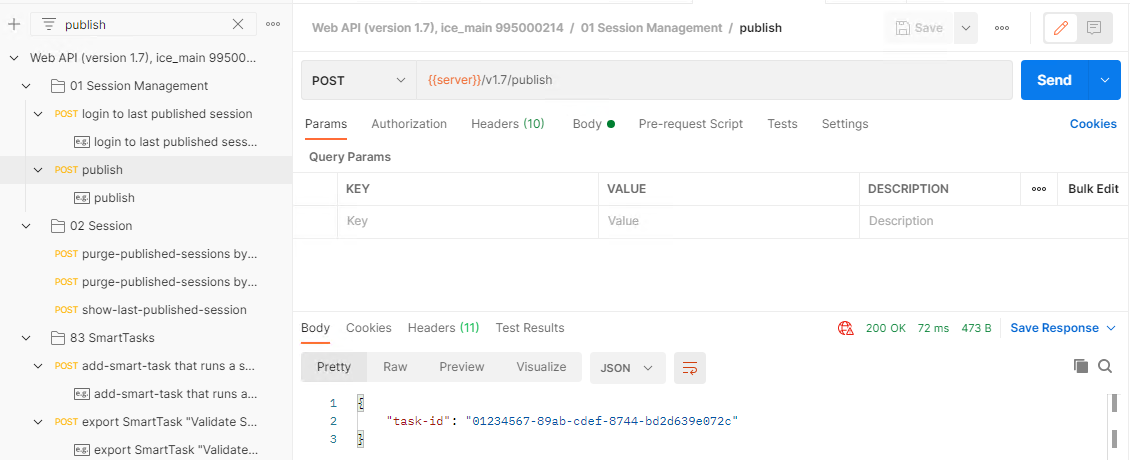
A screenshot of a computer

Description automatically generated

1. Use the filter to find the add-host option in the Postman Collection
2. Review the body of the message that is in the collection. Change the name and IP address to something different if you prefer.



1. Hit the blue Send button and review the status and output from the API server
2. Use the filter to find the publish option and publish your changes

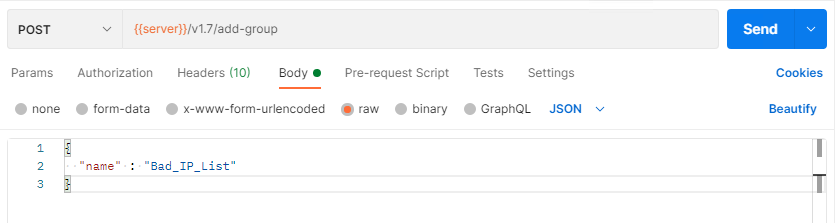


1. Use the filter to find the logout function and logout your session

Task – 3: Create two groups

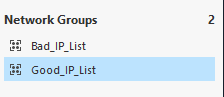
**Objective**: Use Postman and the Management API Guide to create two groups

1. Using what we have learned in Task 2, use Postman to create two groups. A hint is to look at what is required to create a group. A group only requires at a minimum a name to be created.
2. The examples in the Postman collection are based on examples from the API guide.
   1. Create a group called Bad\_IP\_List
   2. Create a group called Good\_IP\_List



|  |  |
| --- | --- |
| 🕮 | *Reminder – The previous session is no longer valid, so login to acquire a new session id!* |

1. Publish your changes



Task – 4: Create a new policy package

**Objective**: Use Postman and the R81 Management API Guide to create a new policy package with section titles

1. Create a new policy package called “API\_Training”. Include Threat Prevention layer.

A screenshot of a computer

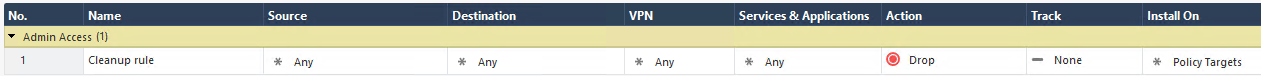
Description automatically generated

|  |  |
| --- | --- |
| 🕮 | *Review the Postman output for the access Layer name. In this case it will typically have Network as the access layer. This will be needed on the next API calls to specify what layer to add section titles to!* |

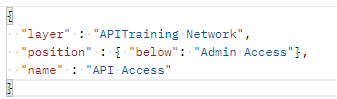
A screenshot of a computer

Description automatically generated

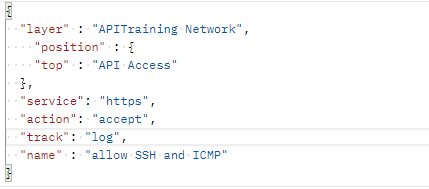
1. Add a new section title on the top called – “Admin Access”.



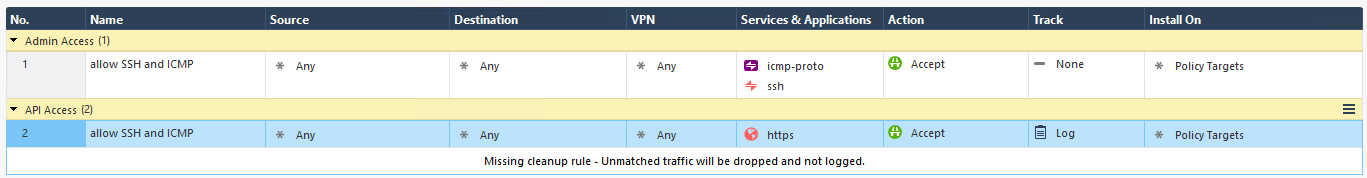
1. Add a new section title below called – “API Access”.



1. Add a new rule in the section “Admin Access” and allow SSH/ICMP-proto from Any/Any/Allow.



1. Add a new rule in the section “API Access” and allow https from Any/Any/Allow.
2. Delete the Cleanup rule.
3. Publish your changes.

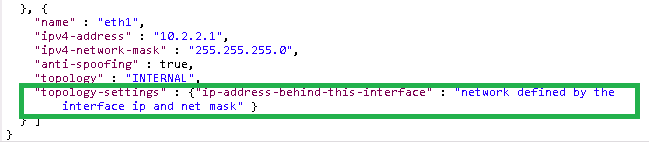


Task – 5: Create a Simple Gateway

**Objective**: Use Postman and the Management API Guide to create a new Simple Security Gateway. Once the gateway is created, modify the API Training Policy as described.

1. Use the following information to create a new Simple Gateway (add-simple-gateway). Check the Postman add-simple-gateway-with-sic as an example. Make sure to remove the sic from the command since the gateway does not really exist.

* Gateway Name: branch\_gw
* Version: R81.20
* Blades – FW, IPS, Antibot, AntiVirus, Threat-Emulation
* Gateway IP: 203.0.113.40
* Interfaces:
  + - Eth0: 203.0.113.40/255.255.255.0
    - Eth1: 10.0.10.40/255.255.255.0
* For eth1 make sure to set the topology correctly for the internal network. Here is an example on what to add.



* Color: Blue

1. Publish your changes.
2. Verify that the gateway shows up in SmartConsole