Routing Security

Deploying RPKI and ROV at Cenpac

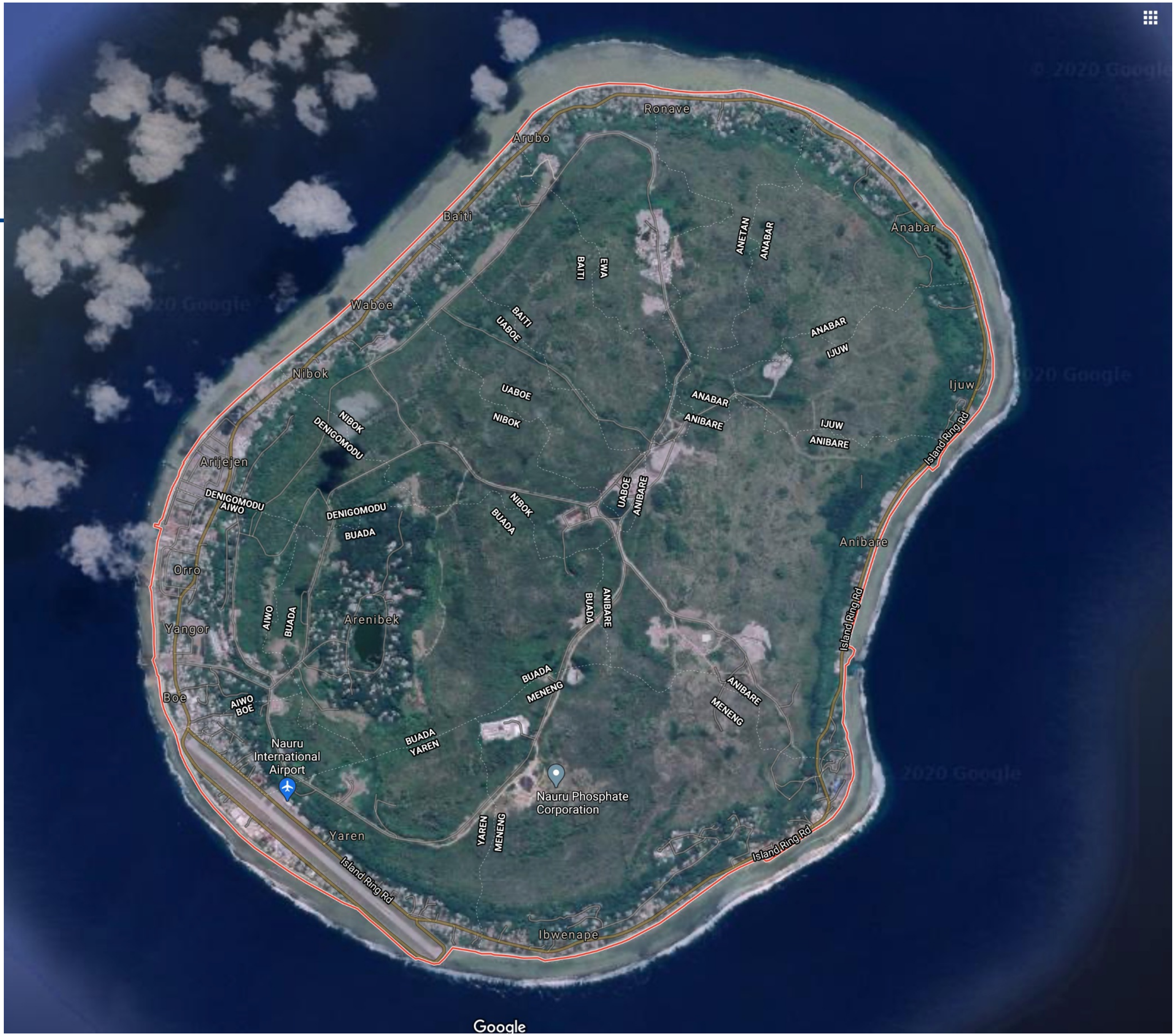
Philip Smith
PFS Internet Development

October 2021

Acknowledgements

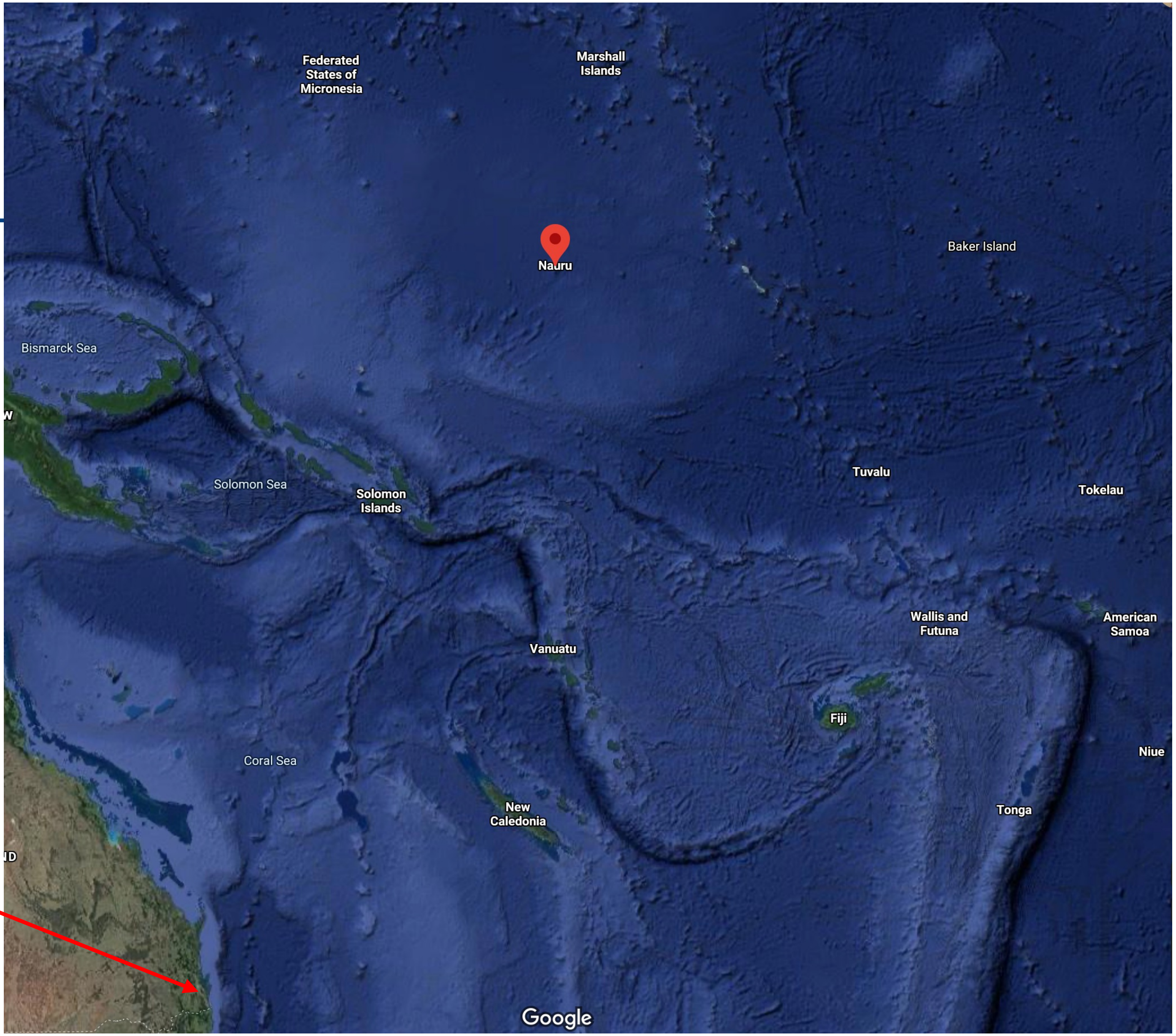
- This presentation documents the work done to deploy RPKI/ROV at CenpacNet on the Pacific Island nation of Nauru
- Thanks to the Network Startup Resource Centre for encouragement and inspiration

Nauru



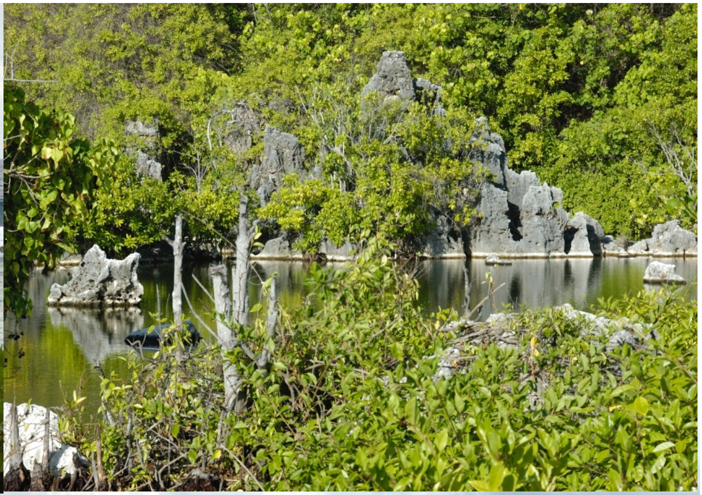
Map by Google

Where?



Brisbane, Australia

Map by Google



Goals

- Why are we doing this?
- Create ROAs covering Nauru address space
- Set up a validator
- Implement Route Origin Validation
- Lessons learned

RPKI status prior to starting

- Two operators serving Nauru:
  - Digicel Nauru
    - Originating 43.230.6.0/24, 103.20.124.0/24, 103.49.173.0/24, 103.49.174.0/23
    - All four prefixes have had ROAs in place for many months
  - Cenpac
    - Originating 203.98.224.0/19 and (in theory) 2403:f600::/32
- One multihomed entity
  - Govt ICT infrastructure
    - Originating 203.98.226.0/23

Why?

- Security of the routing system is important in all its forms
- Cenpac status:
  - For years has done uRPF on all customer facing links (almost pointless as customers all live behind NAT)
  - Created route objects matching announcements (upstream requirement)
  - Filtered inbound and outbound traffic to match Cenpac address space
  - Implementing RPKI seemed obvious next step…

Step 1: Validator

- Create a container on Cenpac's cluster
- Install Routinator 3000 validator
  - Ubuntu package, easy to install and set up
- Watch it for "a while"
  - Many weeks, no reason to wait so long though
- Second validator still to be done
  - One is enough for now though
  - Plan is to create another container running FORT

Step 2: ROV

- Set up the two Border Routers to talk to the validator
- Cisco IOS-XE

```
bgp rpki server tcp 203.98.x.x port 3323 refresh 3600
```

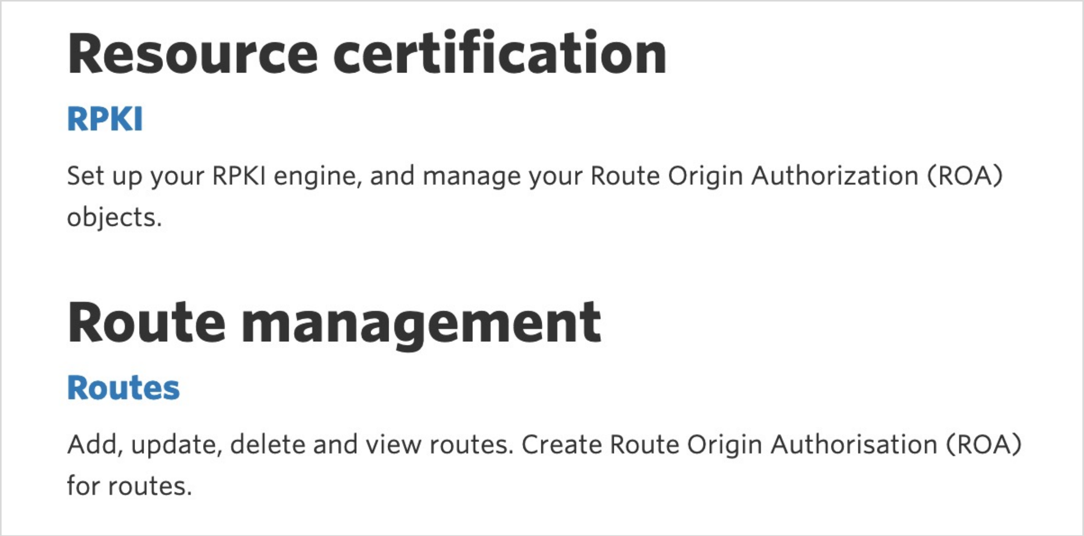
- Easy enough done as well
  - Noting the endless caveats/bugs/problems associated with Cisco’s RPKI implementation 🤯
  - For Cenpac, invalids automatically dropped (Cisco default)
  - Doesn’t matter, as a default route to upstream (satellite) providers required/used
  - Cenpac needs about 50% of the BGP table from one provider to do traffic engineering

Step 3: Signing ROAs

- The hardest part was getting ROAs signed
- Started this two years ago
  - But it was never a priority as there were always other major issues needing resourcing and attention
- Pressure on because Digicel Nauru had already signed address space used in Nauru
  - The one multi-homed customer was also requesting for their address block to be covered by a ROA
- And here’s the story…

Signing ROAs: accessing APNIC member account

- Tech contact needs the Admin contact to "give permission"
  - My access was for Tech only (2FA already done)
- Main Admin contact had account access difficulties as yet unresolved
- Resorted to approaching another Admin contact to set up the needful
- And finally to the MyAPNIC Resource Manager page:



Resource certification

RPKI

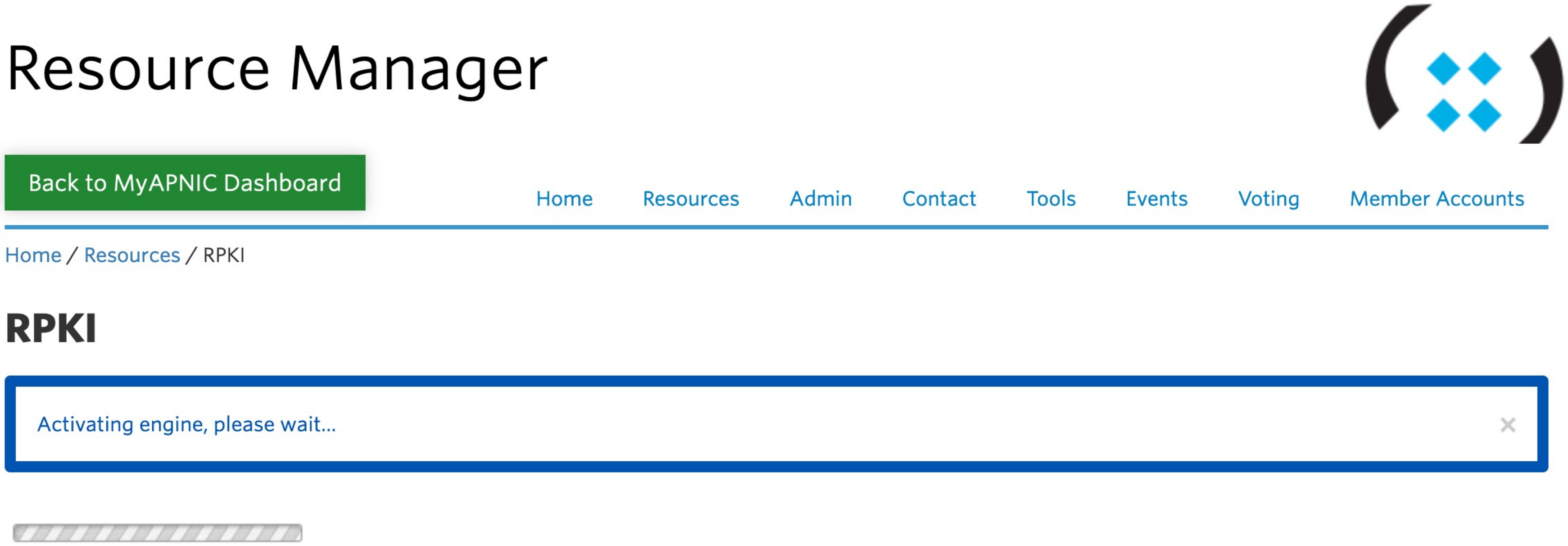
Set up your RPKI engine, and manage your Route Origin Authorization (ROA) objects.

Route management

Routes

Add, update, delete and view routes. Create Route Origin Authorisation (ROA) for routes.

Signing ROAs: enable RPKI engine

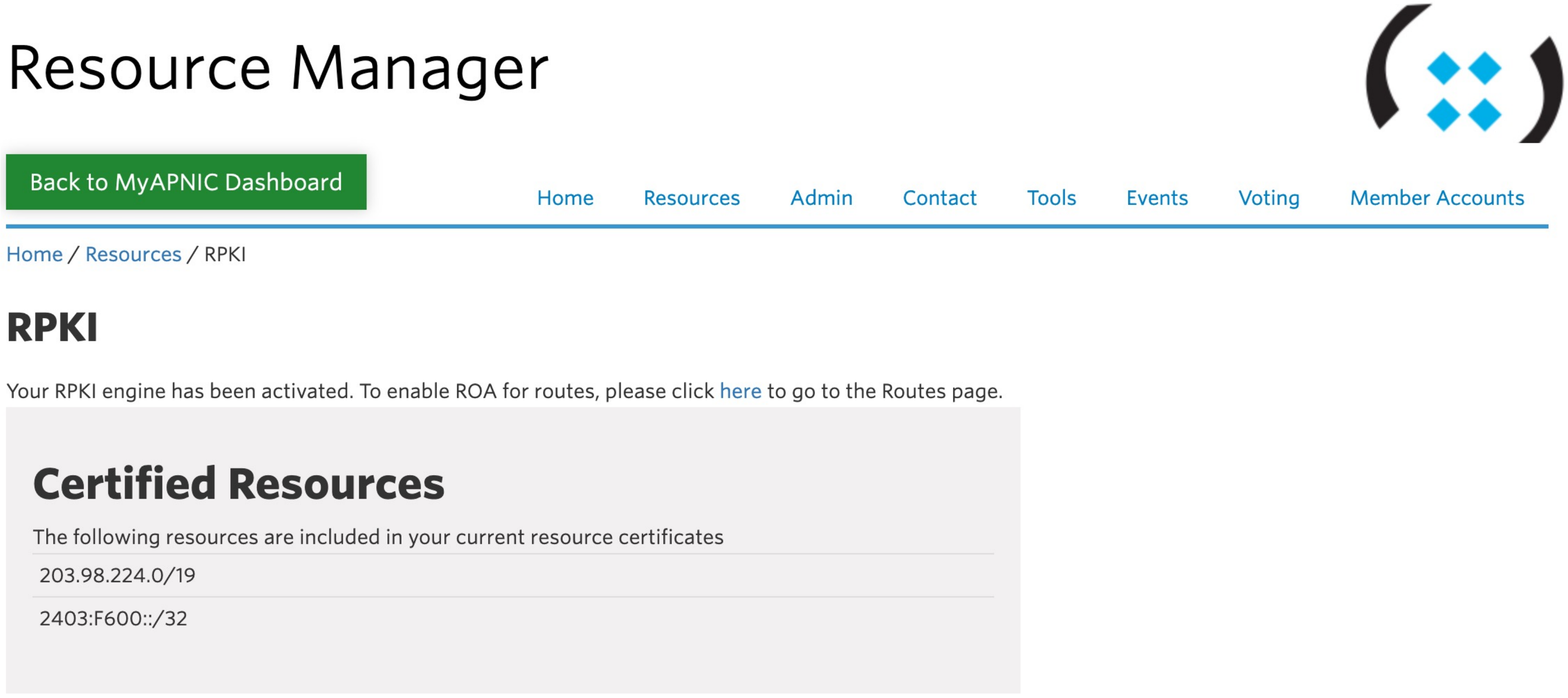


Resource Manager

RPKI

Activating engine, please wait...

Signing ROAs: Resource Manager



Resource Manager

RPKI

Your RPKI engine has been activated. To enable ROA for routes, please click here to go to the Routes page.

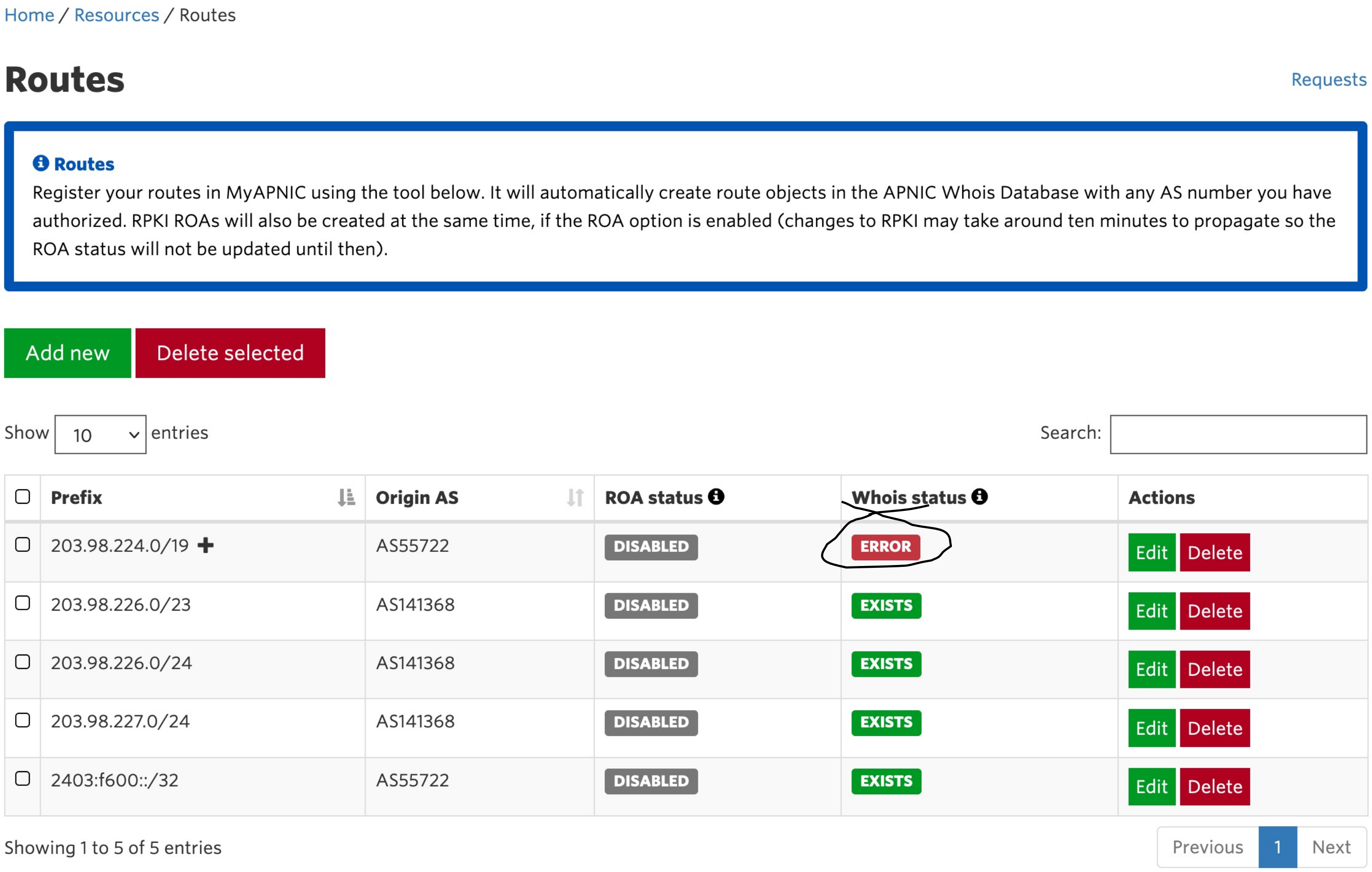
Certified Resources

The following resources are included in your current resource certificates

203.98.224.0/19

2403:F600::/32

Signing ROAs: the Routes page



Home / Resources / Routes

Routes

Requests

Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Show 10 entries

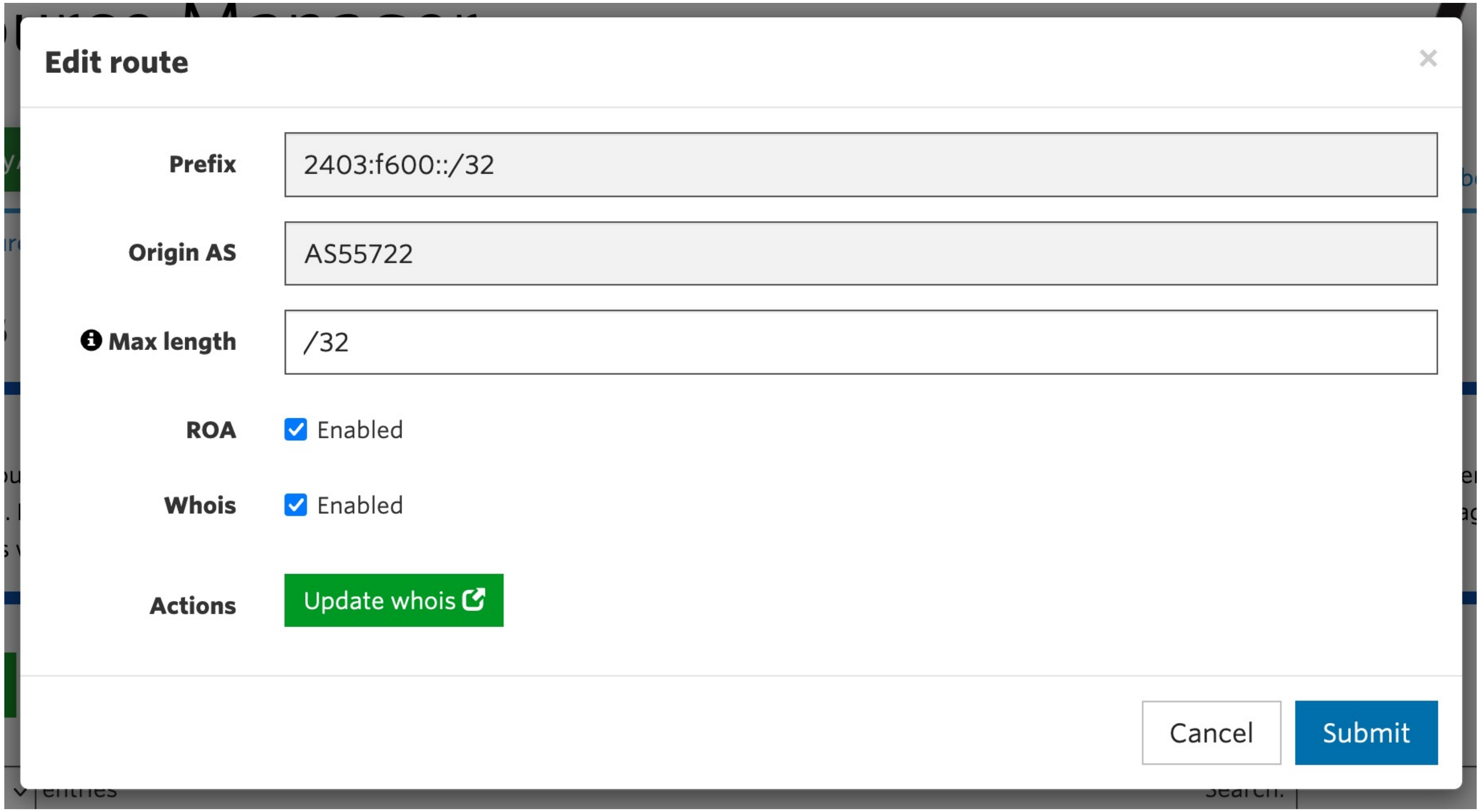
Search:

□	Prefix	Origin AS	ROA status	Whois status	Actions
□	203.98.224.0/19 +	AS55722	DISABLED	ERROR	Edit Delete
□	203.98.226.0/23	AS141368	DISABLED	EXISTS	Edit Delete
□	203.98.226.0/24	AS141368	DISABLED	EXISTS	Edit Delete
□	203.98.227.0/24	AS141368	DISABLED	EXISTS	Edit Delete
□	2403:f600::/32	AS55722	DISABLED	EXISTS	Edit Delete

Showing 1 to 5 of 5 entries

This doesn't look promising

Signing ROAs: IPv6 first

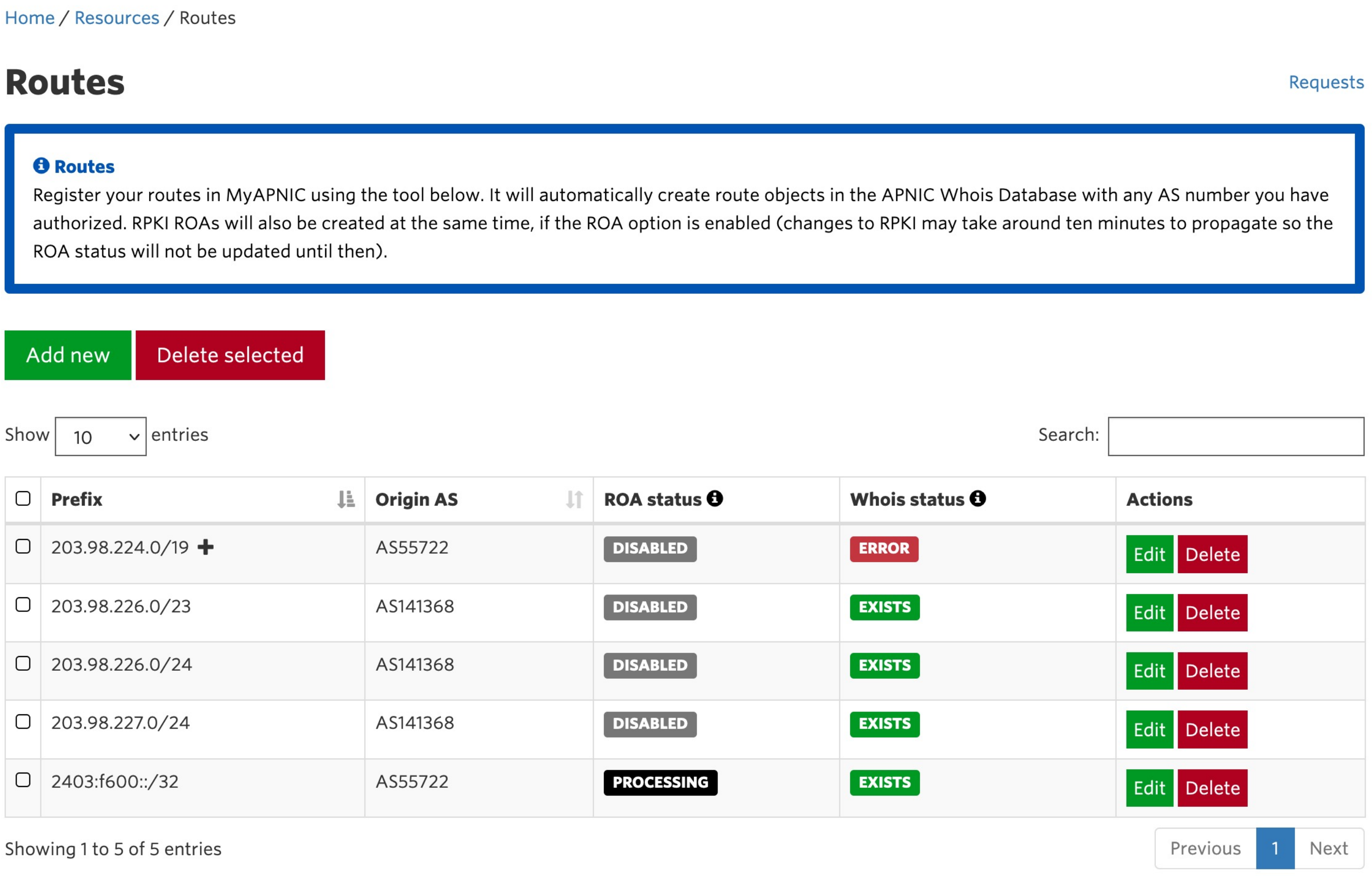


Edit route

Prefix	2403:f600::/32
Origin AS	AS55722
Max length	/32
ROA	☑ Enabled
Whois	☑ Enabled
Actions	Update whois

Create ROA for the IPv6 /32

Signing ROAs: IPv6 first



Home / Resources / Routes

Routes

Requests

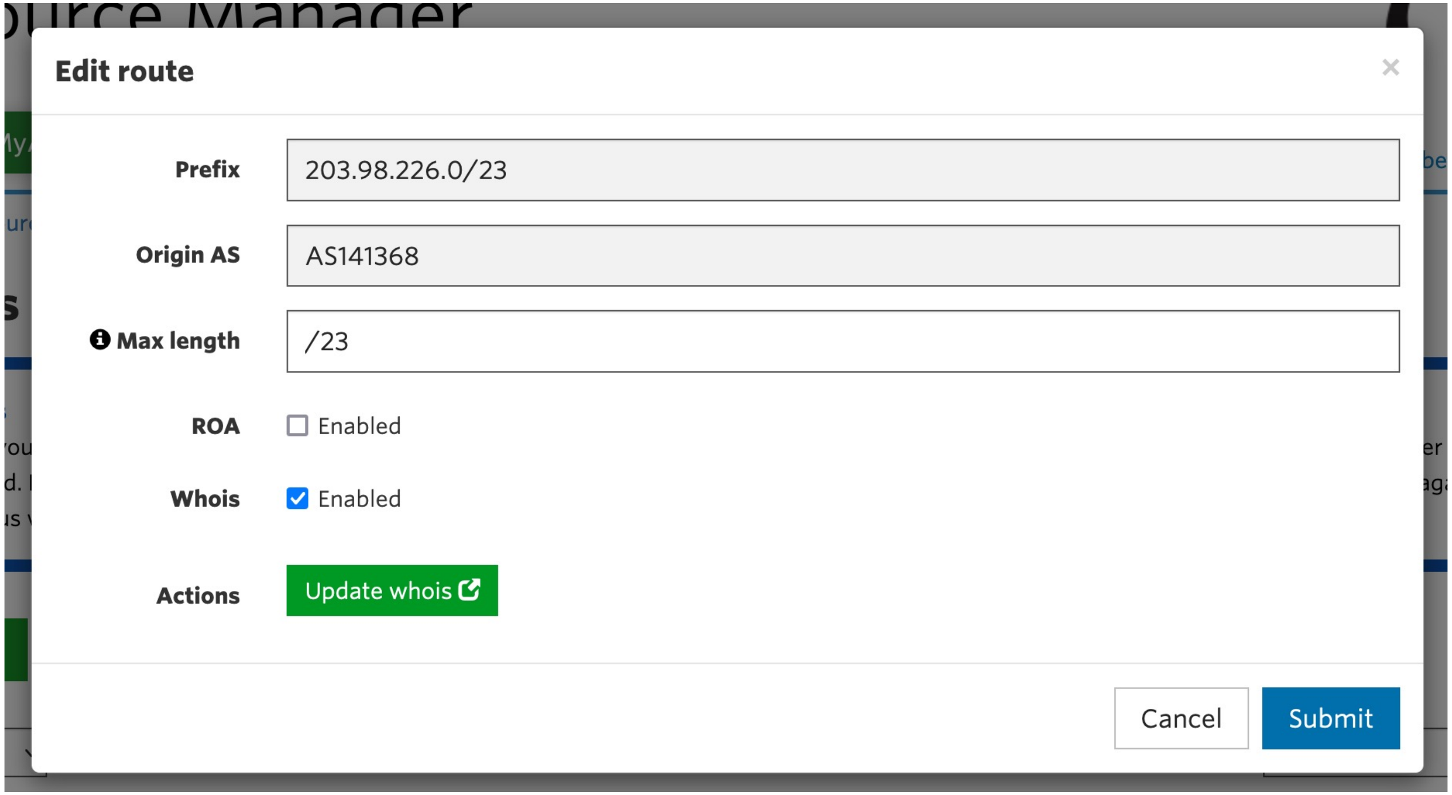
Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

□	Prefix	Origin AS	ROA status	Whois status	Actions
□	203.98.224.0/19 +	AS55722	DISABLED	ERROR	Edit Delete
□	203.98.226.0/23	AS141368	DISABLED	EXISTS	Edit Delete
□	203.98.226.0/24	AS141368	DISABLED	EXISTS	Edit Delete
□	203.98.227.0/24	AS141368	DISABLED	EXISTS	Edit Delete
□	2403:f600::/32	AS55722	PROCESSING	EXISTS	Edit Delete

Showing 1 to 5 of 5 entries

Create ROA for the IPv6 /32

Signing ROAs: multihomed customer



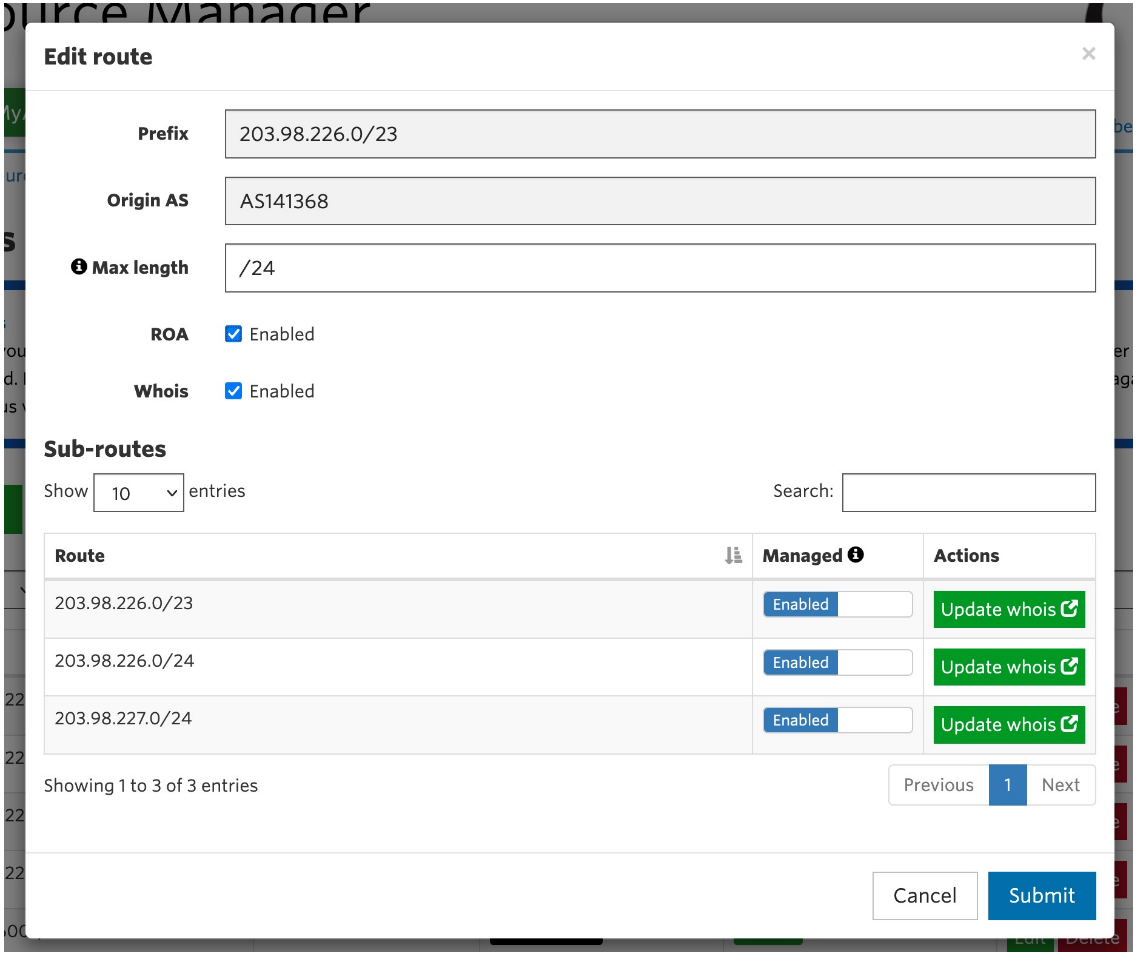
Edit route

Prefix	203.98.226.0/23
Origin AS	AS141368
Max length	/23
ROA	□ Enabled
Whois	☑ Enabled
Actions	Update whois

AS141368 is announcing /23 on both links, with one /24 subnet to one upstream, and the other /24 subnet to the other upstream.

So we need ROA covering the /23 and its two /24s

Signing ROAs: multi-homed customer



Edit route

Prefix	203.98.226.0/23
Origin AS	AS141368
Max length	/24
ROA	☑ Enabled
Whois	☑ Enabled

Sub-routes

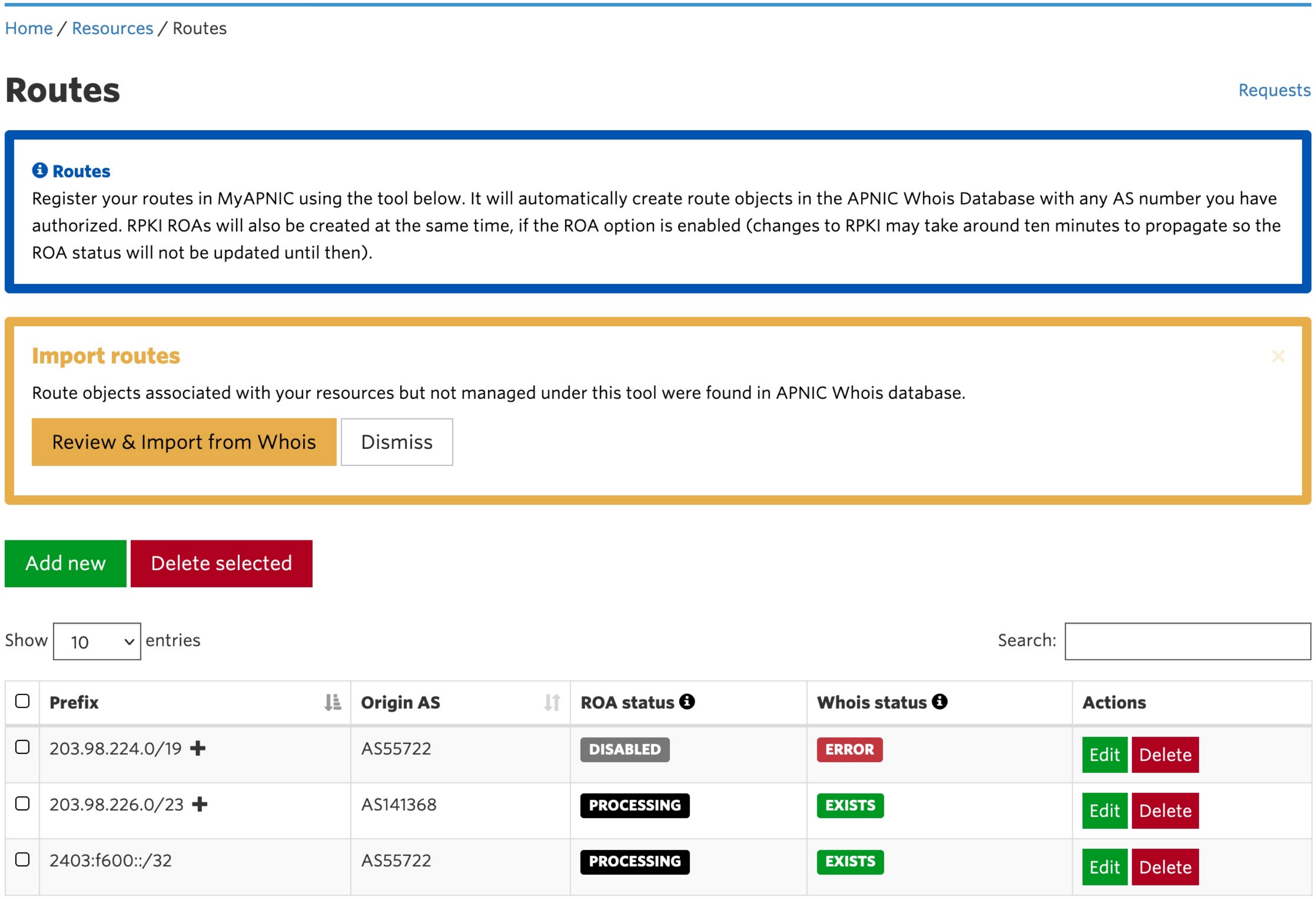
Show 10 entries Search:

Route	Managed	Actions
203.98.226.0/23	Enabled	Update whois
203.98.226.0/24	Enabled	Update whois
203.98.227.0/24	Enabled	Update whois

Showing 1 to 3 of 3 entries

Changing MaxLen to /24 and ticking the "ROA" box changes the screen to this

Signing ROAs: multi-homed customer



Home / Resources / Routes

Routes

Requests

Routes

Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Import routes

Route objects associated with your resources but not managed under this tool were found in APNIC Whois database.

Show 10 entries

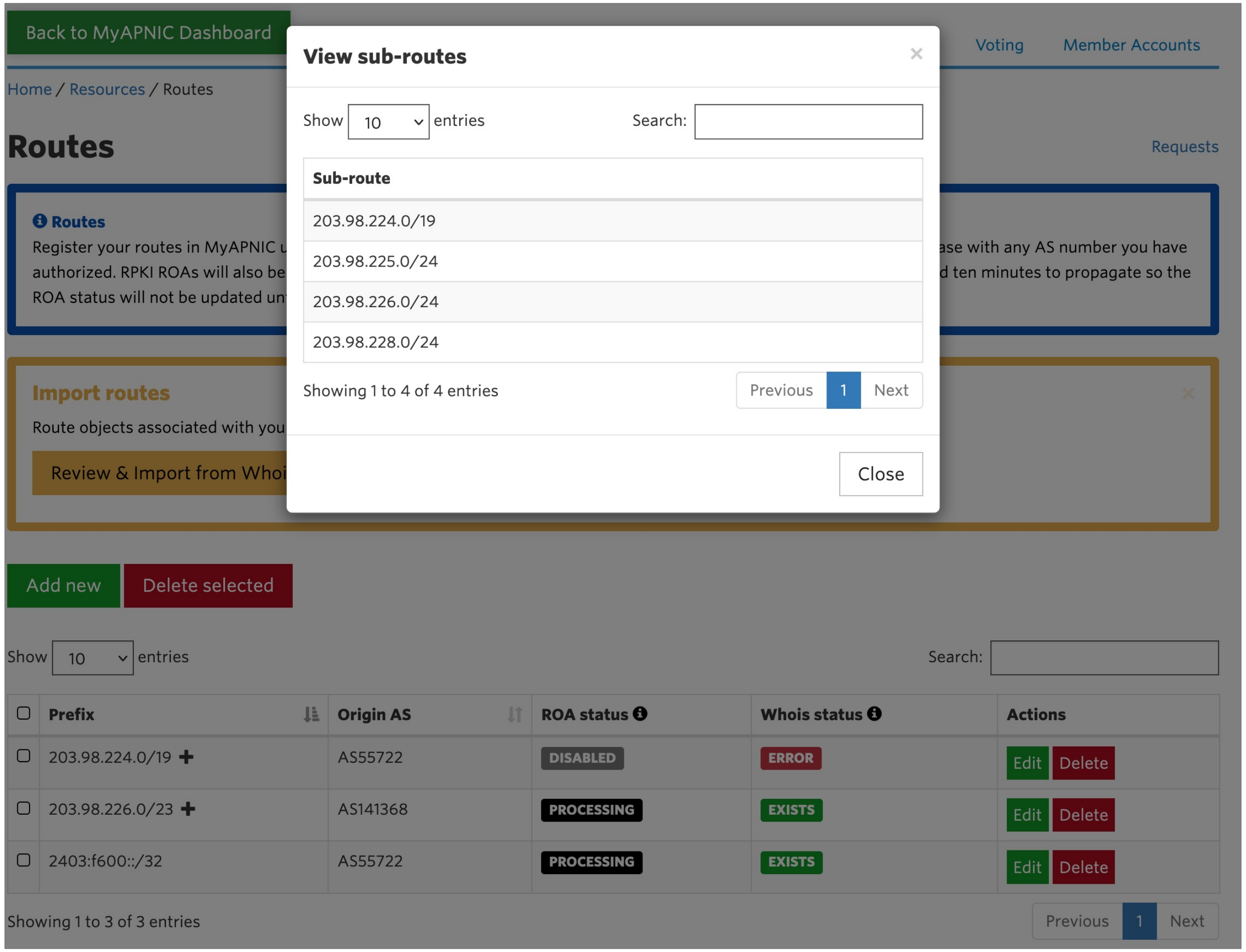
Search:

☐	Prefix	Origin AS	ROA status	Whois status	Actions
☐	203.98.224.0/19 +	AS55722	DISABLED	ERROR	Edit Delete
☐	203.98.226.0/23 +	AS141368	PROCESSING	EXISTS	Edit Delete
☐	2403:f600::/32	AS55722	PROCESSING	EXISTS	Edit Delete

Oh dear, this isn't what I want to see either

My two ROAs are still processing…

Signing ROAs: the orange box



Back to MyAPNIC Dashboard

Voting Member Accounts

Home / Resources / Routes

Routes

Requests

Routes

Register your routes in MyAPNIC u... authorized. RPKI ROAs will also be... ROA status will not be updated un... ...ase with any AS number you have ...d ten minutes to propagate so the

Import routes

Route objects associated with you...

Review & Import from Whoi...

View sub-routes

Show 10 entries Search:

Sub-route
203.98.224.0/19
203.98.225.0/24
203.98.226.0/24
203.98.228.0/24

Showing 1 to 4 of 4 entries

Previous 1 Next

Close

Add new Delete selected

Show 10 entries Search:

☐	Prefix	Origin AS	ROA status	Whois status	Actions
☐	203.98.224.0/19 +	AS55722	DISABLED	ERROR	Edit Delete
☐	203.98.226.0/23 +	AS141368	PROCESSING	EXISTS	Edit Delete
☐	2403:f600::/32	AS55722	PROCESSING	EXISTS	Edit Delete

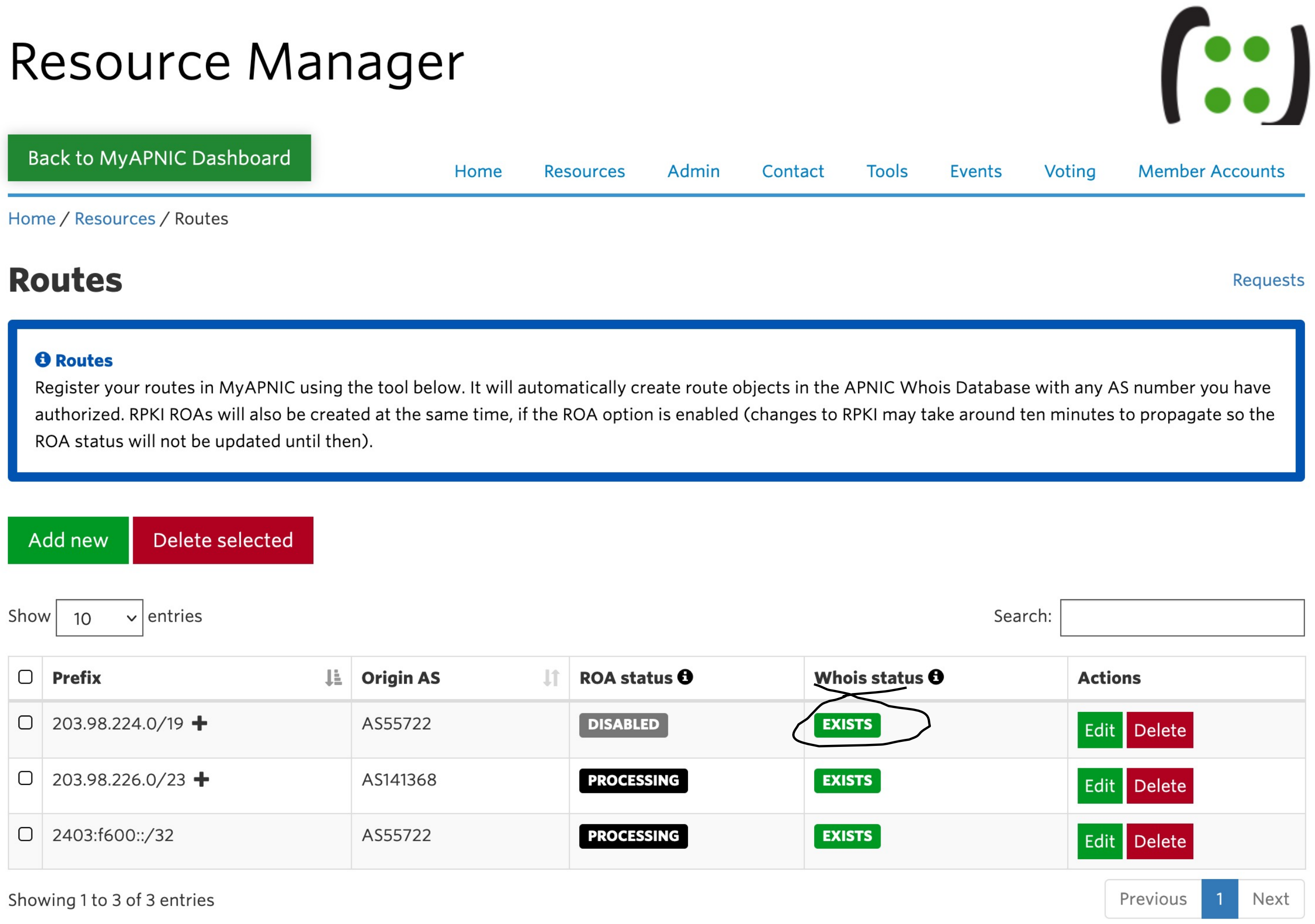
Showing 1 to 3 of 3 entries

Previous 1 Next

These are the existing route objects in the whois database

We can delete those now, as we are going to sign ROAs, and the MyAPNIC tool automatically creates route objects too

Signing ROAs: disappearing errors



Resource Manager

Home / Resources / Routes

Routes

Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Show 10 entries

Search:

☐	Prefix	Origin AS	ROA status	Whois status	Actions
☐	203.98.224.0/19 +	AS55722	DISABLED	EXISTS	Edit Delete
☐	203.98.226.0/23 +	AS141368	PROCESSING	EXISTS	Edit Delete
☐	2403:f600::/32	AS55722	PROCESSING	EXISTS	Edit Delete

Showing 1 to 3 of 3 entries

The error adjacent to 203.98.224.0/19 has now gone! Progress.

Signing ROAs: next, the /19

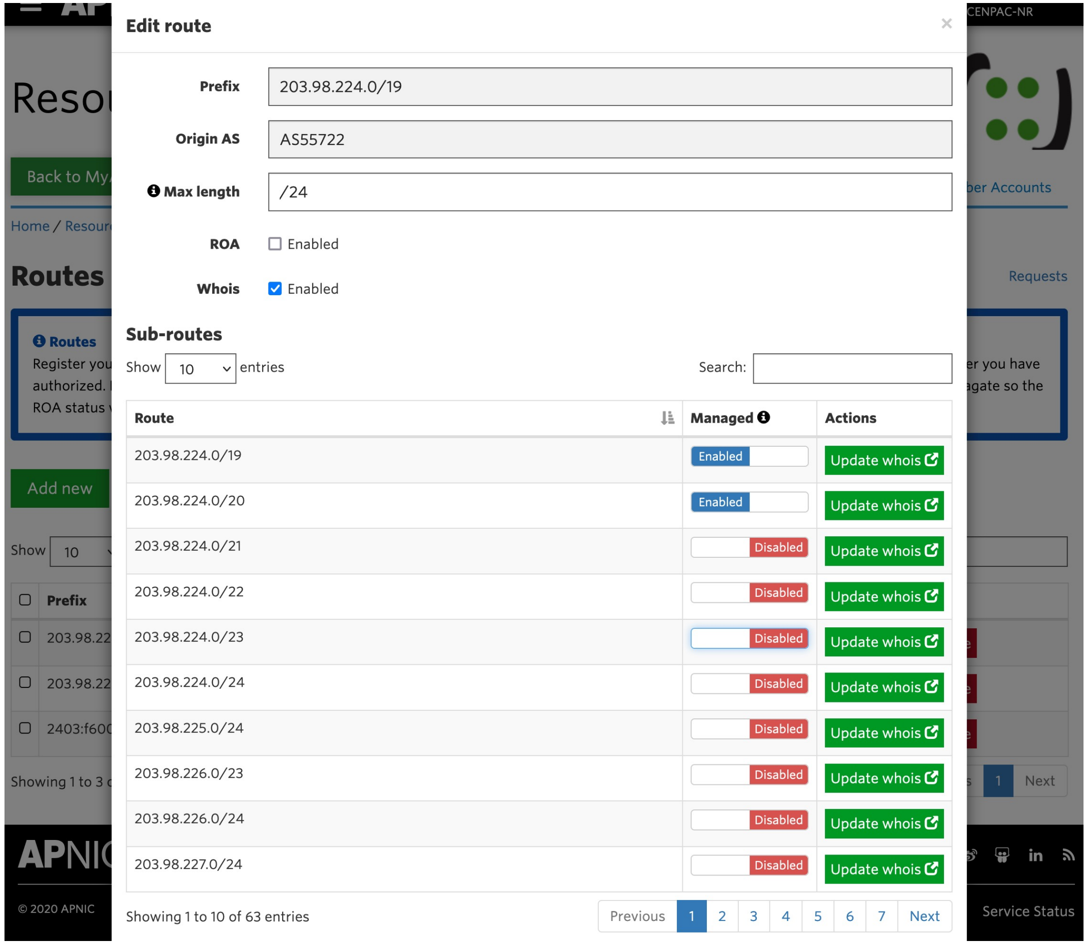
Clicking on **edit** on the previous screen produces this pop-up

And all 7 pages (not shown here)

Yes, MaxLen /24 😬

Is MaxLen /24 chosen by the tool because there are existing route objects for /24s ?

IPv6 MaxLen matched the /32 allocation…



Edit route

Prefix	203.98.224.0/19
Origin AS	AS55722
Max length	/24
ROA	□ Enabled
Whois	☑ Enabled

Sub-routes

Show 10 entries

Search:

Route	Managed	Actions
203.98.224.0/19	Enabled	Update whois
203.98.224.0/20	Enabled	Update whois
203.98.224.0/21	Disabled	Update whois
203.98.224.0/22	Disabled	Update whois
203.98.224.0/23	Disabled	Update whois
203.98.224.0/24	Disabled	Update whois
203.98.225.0/24	Disabled	Update whois
203.98.226.0/23	Disabled	Update whois
203.98.226.0/24	Disabled	Update whois
203.98.227.0/24	Disabled	Update whois

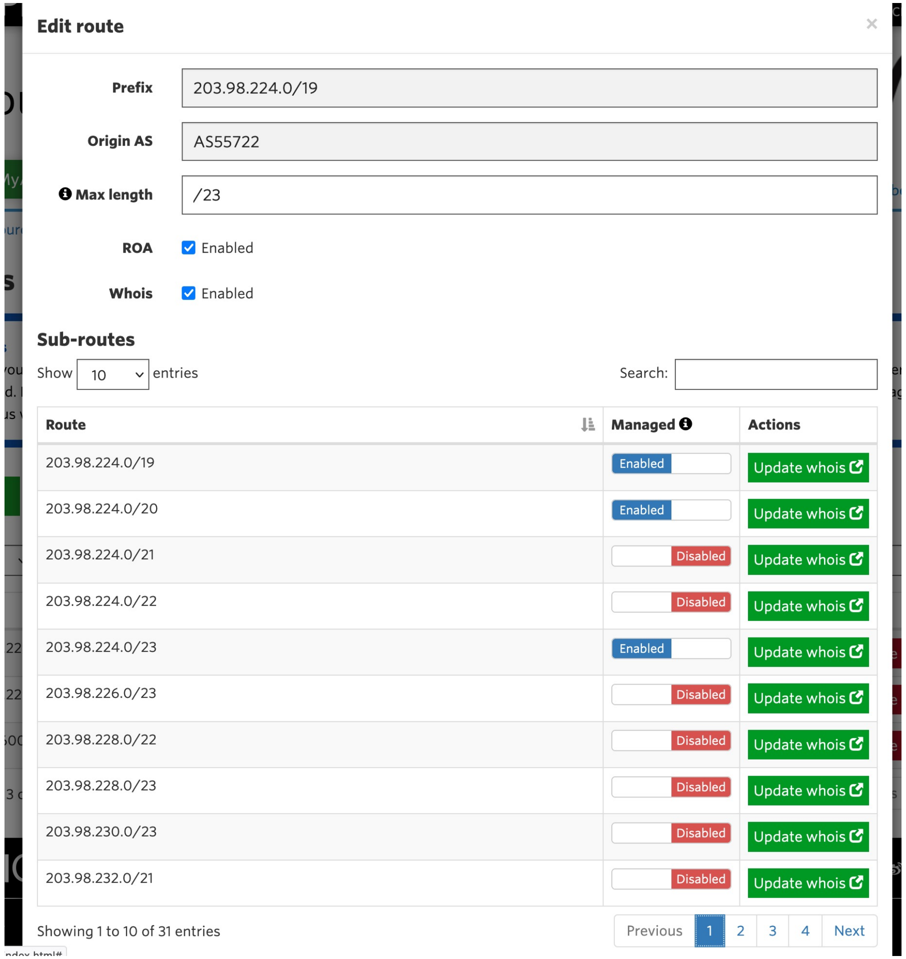
Showing 1 to 10 of 63 entries

Previous 1 2 3 4 5 6 7 Next

Signing ROAs: sorting the /19

Let’s change maxlen to /23, and tag “enabled” for the entries we want ROAs for

Also, tick the ROA box…



Edit route

Prefix: 203.98.224.0/19

Origin AS: AS55722

Max length: /23

ROA: ☑ Enabled

Whois: ☑ Enabled

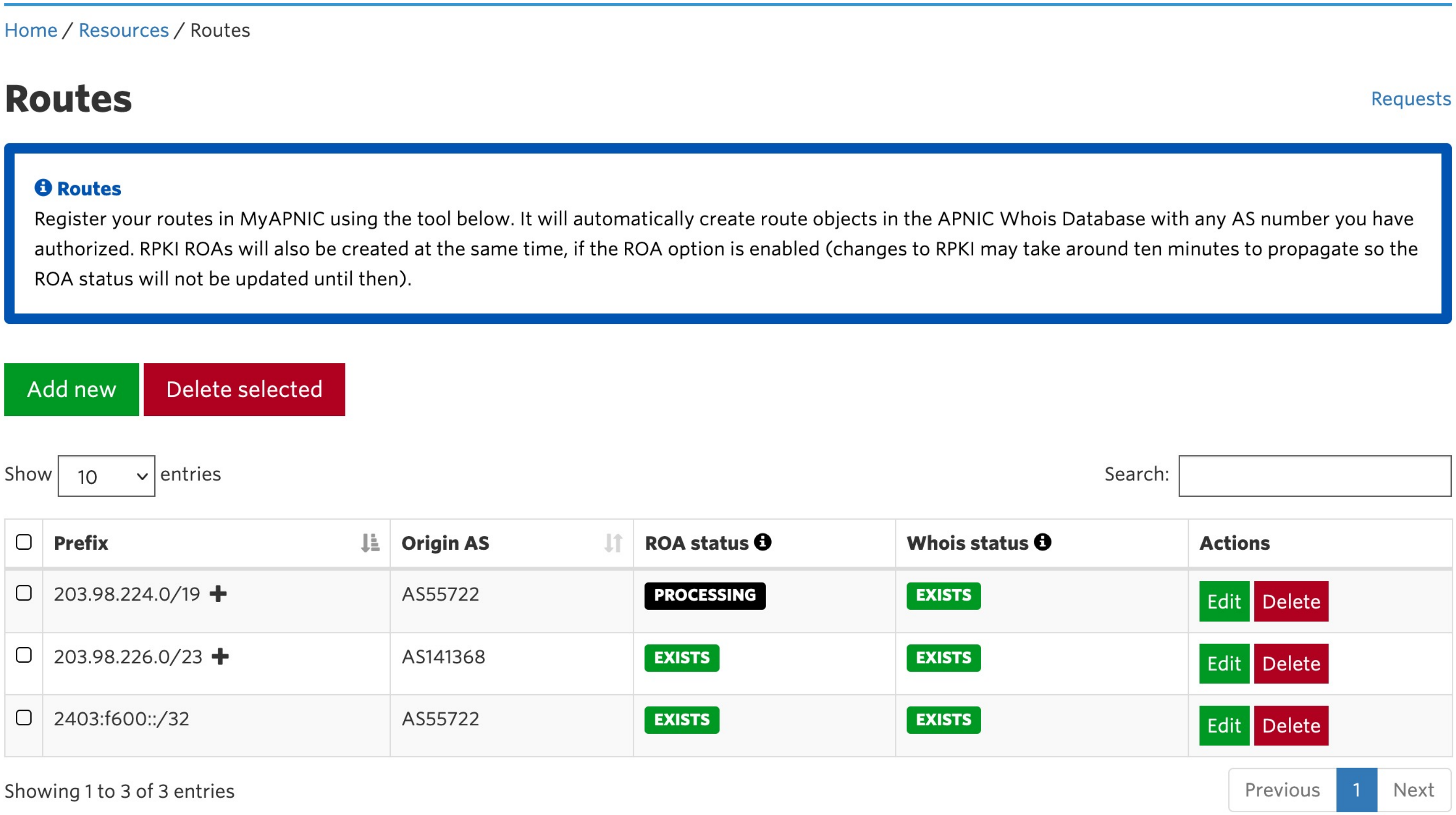
Sub-routes

Show 10 entries — Search:

Route	Managed	Actions
203.98.224.0/19	Enabled	Update whois
203.98.224.0/20	Enabled	Update whois
203.98.224.0/21	Disabled	Update whois
203.98.224.0/22	Disabled	Update whois
203.98.224.0/23	Enabled	Update whois
203.98.226.0/23	Disabled	Update whois
203.98.228.0/22	Disabled	Update whois
203.98.228.0/23	Disabled	Update whois
203.98.230.0/23	Disabled	Update whois
203.98.232.0/21	Disabled	Update whois

Showing 1 to 10 of 31 entries

Signing ROAs: sorting the /19



Home / Resources / Routes

Routes

Requests

Routes

Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

Add new | Delete selected

Show 10 entries

Search:

□	Prefix	Origin AS	ROA status	Whois status	Actions
□	203.98.224.0/19 +	AS55722	PROCESSING	EXISTS	Edit Delete
□	203.98.226.0/23 +	AS141368	EXISTS	EXISTS	Edit Delete
□	2403:f600::/32	AS55722	EXISTS	EXISTS	Edit Delete

Showing 1 to 3 of 3 entries

Previous 1 Next

Looks promising…

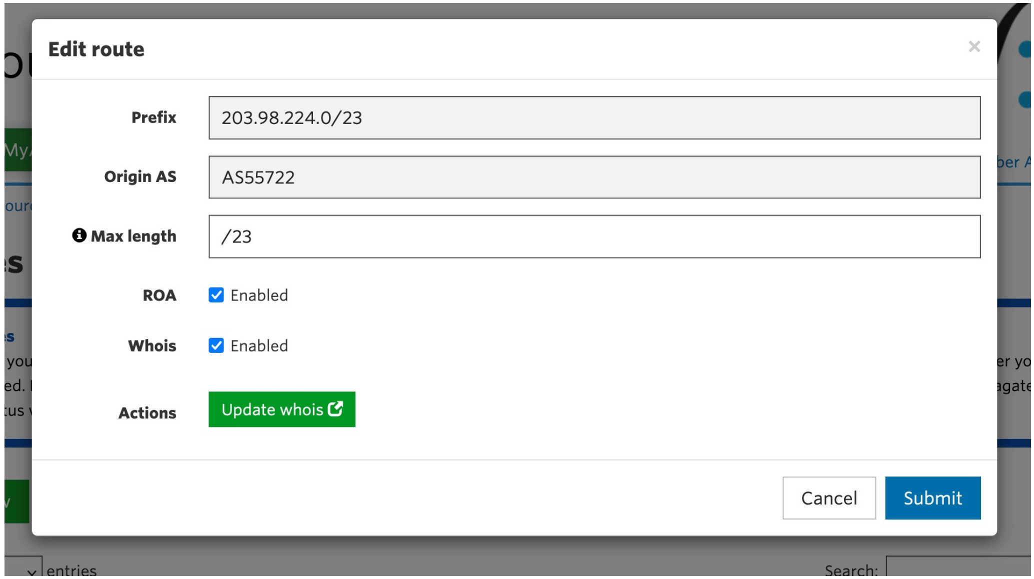
But it failed… 🤯

Signing ROAs: the problem

- Two slides back the 203.98.224.0/19 screen showed every single subnet of the /19
- All I wanted to do was create ROAs for:
  - 203.98.224.0/19
  - 203.98.224.0/20 (traffic engineering)
  - 203.98.240.0/20 (traffic engineering)
  - 203.98.224.0/23 (traffic engineering)
- And that is not done by setting max-len of /23 and then enabling or disabling subnets as the pages might suggest

Signing ROAs

- The solution:
  - Create entries on route page for:
    - 203.98.224.0/19 with max-len of 20
    - 203.98.224.0/23 with max-len of 23



Edit route

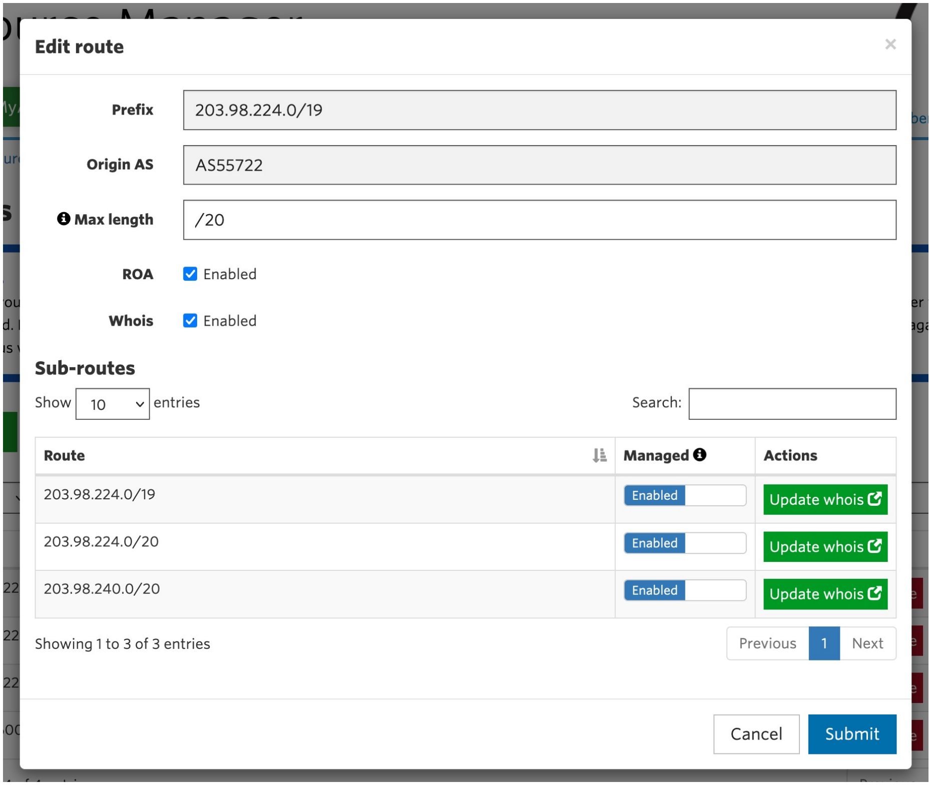
Prefix: 203.98.224.0/23

Origin AS: AS55722

Max length: /23

ROA: ☑ Enabled

Whois: ☑ Enabled



Edit route

Prefix: 203.98.224.0/19

Origin AS: AS55722

Max length: /20

ROA: ☑ Enabled

Whois: ☑ Enabled

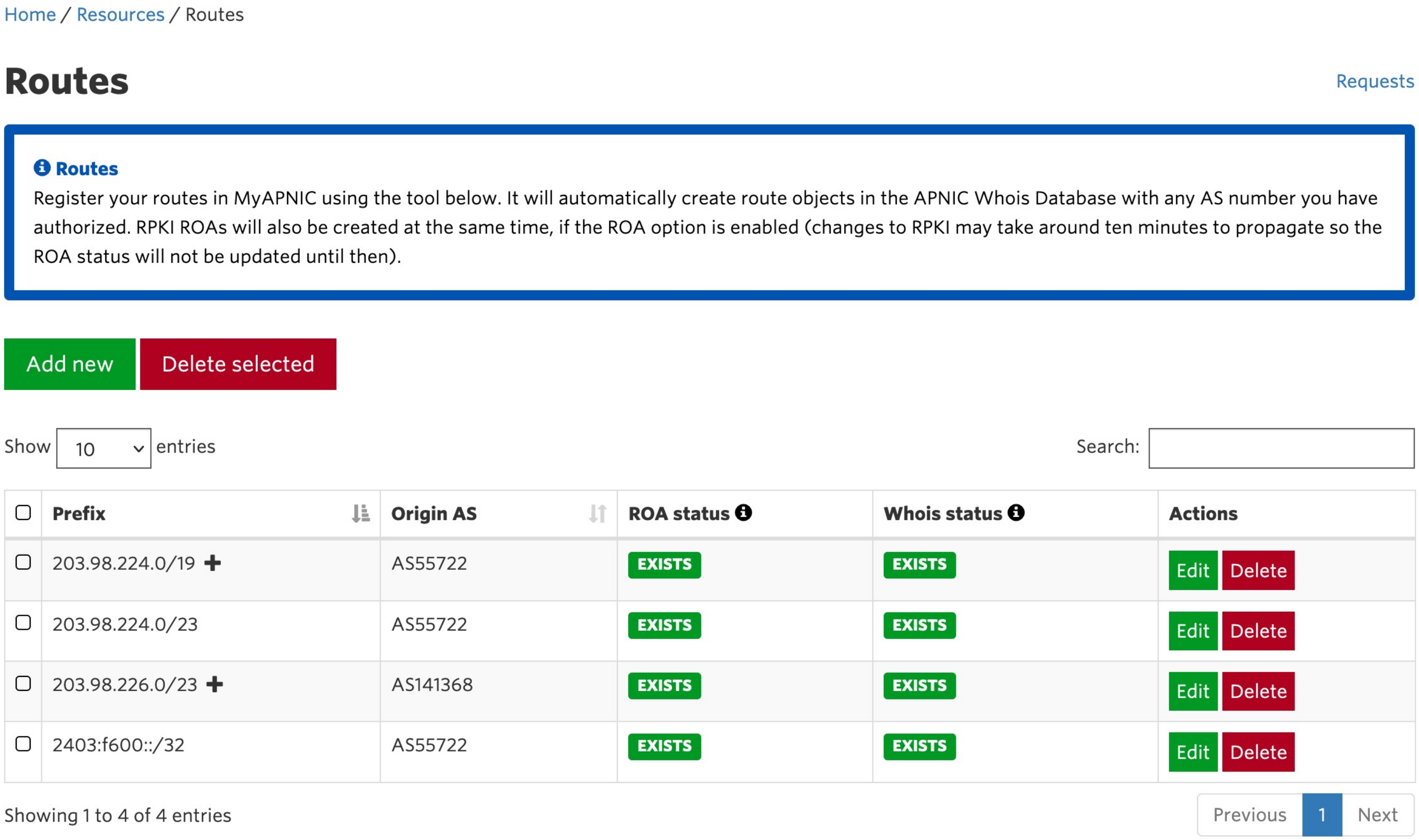
Sub-routes

Show 10 entries Search:

Route	Managed	Actions
203.98.224.0/19	Enabled	Update whois
203.98.224.0/20	Enabled	Update whois
203.98.240.0/20	Enabled	Update whois

Showing 1 to 3 of 3 entries

Signing ROAs: success!



Home / Resources / Routes

Routes

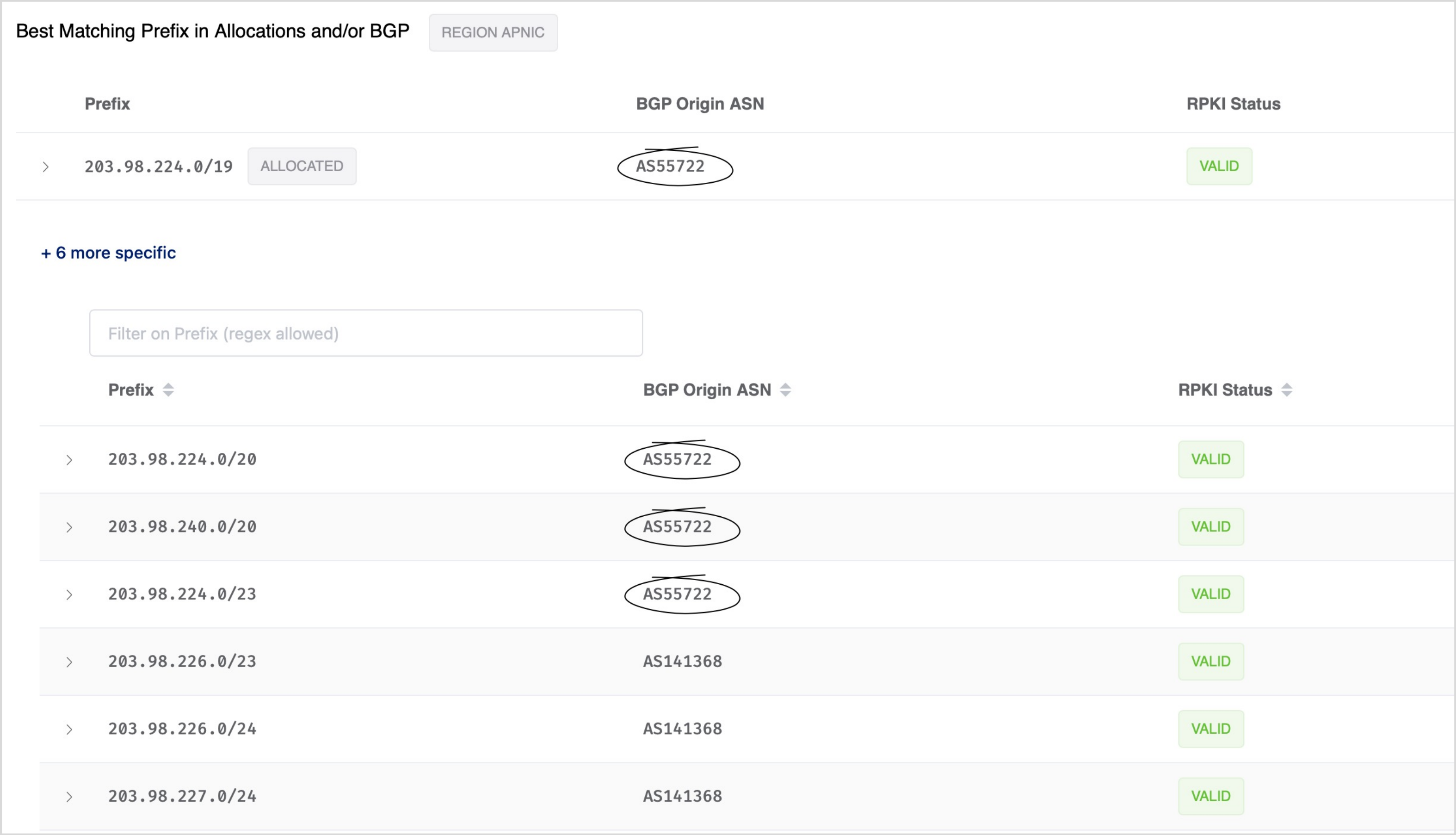
Requests

Routes
Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around ten minutes to propagate so the ROA status will not be updated until then).

□	Prefix	Origin AS	ROA status	Whois status	Actions
□	203.98.224.0/19 +	AS55722	EXISTS	EXISTS	Edit Delete
□	203.98.224.0/23	AS55722	EXISTS	EXISTS	Edit Delete
□	203.98.226.0/23 +	AS141368	EXISTS	EXISTS	Edit Delete
□	2403:f600::/32	AS55722	EXISTS	EXISTS	Edit Delete

Showing 1 to 4 of 4 entries

Routinator web interface summary



Best Matching Prefix in Allocations and/or BGP REGION APNIC

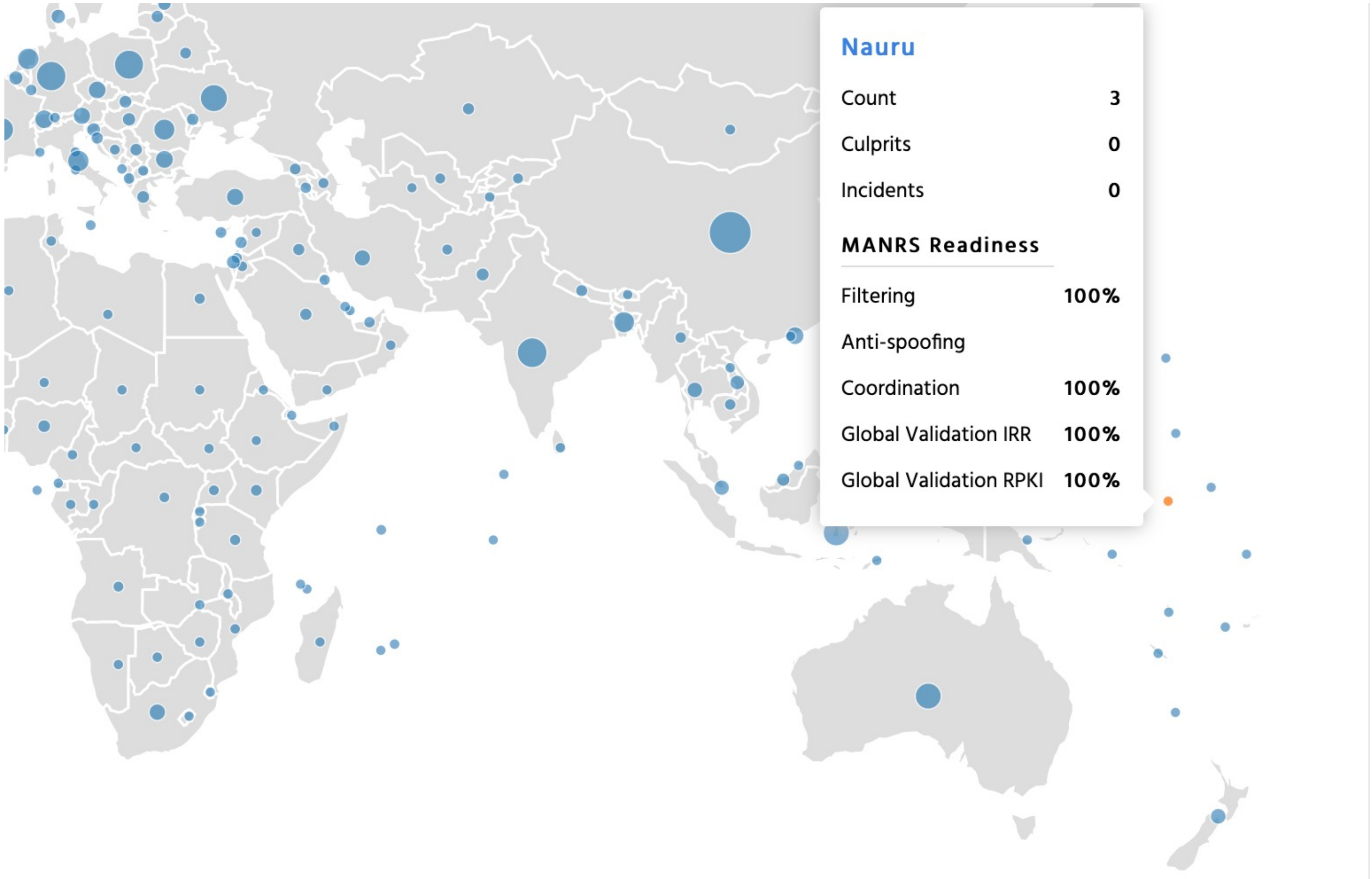
Prefix	BGP Origin ASN	RPKI Status
203.98.224.0/19 ALLOCATED	AS55722	VALID

+ 6 more specific

Filter on Prefix (regex allowed)

Prefix	BGP Origin ASN	RPKI Status
203.98.224.0/20	AS55722	VALID
203.98.240.0/20	AS55722	VALID
203.98.224.0/23	AS55722	VALID
203.98.226.0/23	AS141368	VALID
203.98.226.0/24	AS141368	VALID
203.98.227.0/24	AS141368	VALID

MANRS Observatory: 100%



Nauru

Count	3
Culprits	0
Incidents	0

MANRS Readiness

Filtering	100%
Anti-spoofing	
Coordination	100%
Global Validation IRR	100%
Global Validation RPKI	100%

Lessons: routing security

- uRPF is simple to do
- Inbound/outbound packet filtering is simple to do
- Keeping IRR objects updated also is straightforward
  - Cenpac is APNIC member, therefore APNIC IRR is used

- But we’ve known how to do these for at least 20 years!

Lessons: ROV

- For edge operator outside default free zone, mostly academic exercise
  - Still, I'm curious to see…
  - …and still think of null routing the exact invalid…
- Routinator 3000 is easiest to get up and running
  - Hint to others – if it's not "apt install" or "snap install" or "yum install" do you really expect the average busy netops to waste time installing a development environment and dependencies just to build it?
- Cisco IOS-XE long term bugs/misfeatures that simply aren't being addressed
  - How to fix Cisco?

Lessons: creating ROAs

- Admin/Tech contact access is crucial
  - Admin contact does administration, yet granting RPKI capability is “technical”, causing challenges
    - Open question: is the tech contact untrustworthy?
    - And if so, why are they the tech contact then?
  - 2FA needed, and for some admin folks this is their first encounter!
  - Lands in “too complicated bucket”
    - Here: Tech contact given Admin access
    - Is this really what we want? → Rethink needed

Lessons: creating ROAs

- The steps for creating ROAs in the presence of existing whois entries is confusing:
  - The MyAPNIC UI is not intuitive
    - The “orange box” of existing whois entries isn’t helpful
    - “Review and Import” does not help in the way intended
    - MaxLen confusion
  - To reduce pain:
    - Work on one allocation at a time!
    - Note all existing route objects for the allocation
      - Then delete them! (Don’t worry, they return when ROAs are created)
    - Create ROAs for what is announced, no more (careful with MaxLen)

Thank you!