

[New issue](#)[Jump to bottom](#)

## Can add custom ports without permission #443

🔒 Closed🔄 3 tasks done

Fabrimat opened this issue on Apr 24, 2021 · 5 comments

Assignees



Labels

core

promoted

security

Projects

AMP Core

Fabrimat commented on Apr 24, 2021 • edited

### Bug Report

#### System Information

- Operating System 4.19.0-16-amd64 SMP Debian 4.19.181-1 (2021-03-19) x86\_64 GNU/Linux
- AMP version and build date v2.1.0.14, built 08/04/2021 18:11
- Which AMP release stream you're using Mainline

#### I confirm:

- ☒ that I have searched for an existing bug report for this issue.
- ☒ that I am using the latest available version of AMP.
- ☒ that my operating system is up-to-date.

#### Symptoms

- What are you trying to do?  
Editing ports of an instance without having the proper permission
- What are you expecting to happen?  
That it gives me an error
- What is actually happening? ('Nothing' is not an acceptable answer!)  
The port is added without saying anything

#### Reproduction

1. I created a Minecraft instance with those settings

### Settings for instance Test

Friendly Name	Description
Test	
Start on Boot	Suspended
<input checked="" type="checkbox"/> On	<input type="checkbox"/> Off
Whether or not this instance should start automatically when the system boots.	Suspended instances cannot be accessed and prompt the user to contact the administrator.
Exclude From Firewall	Run in Docker Container
<input checked="" type="checkbox"/> On	<input checked="" type="checkbox"/> On
If set, this instance will <i>not</i> have firewall rules generated for it.	Instances in Docker containers are isolated from other instances and the rest of the system, at the expense of a minor performance impact.
Container Memory Policy	Container Memory (MB)
Unspecified	0
	If the memory policy is 'reserve', how much memory should be set aside for this container as a minimum. If the memory policy is 'restrict', how much memory this container may use maximum. Setting to 0 results in no limit.
Container CPUs	0
The maximum number of CPU shares that this container may use. Roughly matches up with the number of CPU cores/threads the container can use but non-multithreaded applications may not see performance increases from higher values. Setting to 0 results in no limit.	
<button>Close</button>	<button>Save Changes</button>

2. Created a Test user with the following permissions (the user is not member of any group)

Permissions for Test

User specific permissions for Test

This role is shared across all instances.

- Settings
  - Which Settings users in this role have permission to change the value of
- AMP Instance Manager
- File Manager
- Local File Backup
- AMPCore
  - Core functionality built into AMP itself
- All Instances
  - Local Instances
    - Test
      - Start
      - Stop
      - Restart
      - Update
      - Manage

3. Login with a super admin and check the instance ports

Port usage for Test

Description	Port Number	Protocol
SFTP Port Number FileManagerPlugin.SFTPSFTPPortNumber	2224	TCP
Port Number MinecraftModule.Minecraft.PortNumber	25565	TCP+UDP
Add Custom Port		
	1025	TCP

Close Save Changes

4. Login with the Test user, click on the Minecraft Instance and then "Edit ports"

Test

Instances

Main Menu

- Instances
- Configuration

Local Instances

Test

Module: Minecraft

Endpoint: 127.0.0.1:8081

Autostart: Yes

Status: Running

Port usage for Test

Description	Port Number	Protocol
Add Custom Port		
	1025	TCP

Close Save Changes

Test

Instance Name: Test

Friendly Name: Test

Description: Yes

Running: Yes

Module: Minecraft

Binding: 127.0.0.1:8081

Endpoint: 0.0.0.0:25565

Management Mode: Managed by ADS

Start on Boot: Yes

Suspended: No

Actions

Stop Instance Manage

Edit Settings Edit Ports

Update Delete Instance

5. Click on the "+" in the dialog and then "Close"

6. Check again the ports with the super admin

Port usage for Test

Description	Port Number	Protocol
SFTP Port Number FileManagerPlugin.SFTPSFTPPortNumber	2224	TCP
Port Number MinecraftModule.Minecraft.PortNumber	25565	TCP+UDP
CustomPort	1025	TCP
Add Custom Port		
	1025	TCP

Close Save Changes

7. A new port has been added

On the step 5, if I do "Save changes" it will give me this error

## Unable to reconfigure instance

You do not have permission to use this method (ADSMModule.SetInstanceNetworkInfo) at this time. This method requires the ADS.InstanceManagement.Reconfigure permission.

OK


PhonicUK commented on Apr 28, 2021 • edited

Contributor

Clicking + doesn't actually add the port, the network changes aren't applied until you actually hit "Save". If you fully reload the page they won't be there.

It might be incorrectly showing that they're in the list (and it shouldn't be showing the option to edit ports if you don't have permission) - but I can verify that the security model is operating correctly and the changes are not being applied when the user doesn't have permission. Indeed as it says, the API call to set the network information (the ports) requires the global Reconfigure permission for ADS.

So while it's a tad confusing that the user can even see that dialog when they won't be able to make any changes, the security model is operating as intended and there is no fault.

 PhonicUK closed this as completed on Apr 28, 2021

Fabrimat commented on Apr 28, 2021 • edited

Author

As I stated in the report, I can see the port using a different user, I forget to say that is was also with a different browser.  
Also, clicking + apply immediately the changes, if i then press "Close" and then CTRL+F5 and check again the port it's still there.  
Also, using the network analyzer included in the browser I can see this clicking the +:

▼ POST

Scheme: https  
Host: [REDACTED]  
Filename: /API/ADSMModule/ModifyCustomFirewallRule  
Address: [REDACTED]

Status: 200 OK ⓘ  
Version: HTTP/2  
Transferred: 253 B (26 B size)  
Referrer Policy: strict-origin-when-cross-origin

Headers Cookies Request Response Timings Stack Trace Security

Filter Request Parameters

▼ Form data

("InstanceID":"06632f8e-2659-4cec-b541-f810063d8f25";PortNumber:1025;Range:1;Protocol:0;Description:"";Open:true;SESSIONID:"3246e826-8fec-4bb9-8568-30d01f9b4d75"); ""

Headers Cookies Request Response

Filter properties

▼ JSON

▼ result: Object ( Status: true )

Status: true

And right after:

▼ POST

Scheme: https  
Host: [REDACTED]  
Filename: /API/ADSMModule/GetInstanceNetworkInfo  
Address: [REDACTED]

Status: 200 OK ⓘ  
Version: HTTP/2  
Transferred: 713 B (485 B size)  
Referrer Policy: strict-origin-when-cross-origin

Headers Cookies Request Response Timings Stack Trace Security

Filter properties

▼ JSON

▼ result: [ { }, { }, { } ]

▼ 0: Object ( PortNumber: 2236, Protocol: 0, ProvisionNodeName: "FileManagerPlugin.SFTP.SFTPPortNumber", ... )

PortNumber: 2236  
Protocol: 0  
ProvisionNodeName: "FileManagerPlugin.SFTP.SFTPPortNumber"  
Verified: true  
Description: "SFTP Port Number"  
Range: 1  
IsUserDefined: false

▼ 1: Object ( PortNumber: 25566, Protocol: 2, ProvisionNodeName: "MinecraftModule.Minecraft.PortNumber", ... )

PortNumber: 25566  
Protocol: 2  
ProvisionNodeName: "MinecraftModule.Minecraft.PortNumber"  
Verified: true  
Description: "Port Number"  
Range: 1  
IsUserDefined: false

▼ 2: Object ( PortNumber: 1025, Protocol: 0, ProvisionNodeName: "CustomPort", ... )


PortNumber: 1025  
Protocol: 0  
ProvisionNodeName: "CustomPort"  
Verified: true  
Description: ""  
Range: 1  
IsUserDefined: true

 PhonicUK reopened this on Apr 30, 2021

PhonicUK commented on Apr 30, 2021

Contributor

Aah, there was a change at one point where the + and - didn't actually make the changes, indeed you're right and at the moment they do. Different API calls in that situation. Turns out, `ModifyCustomFirewallRule` was missing the metadata for its permissions because originally it wasn't exposed to the web. Not a huge issue since you'd have to at least be logged in, but this will be patched immediately.

 PhonicUK closed this as completed on Apr 30, 2021

 PhonicUK added core promoted security labels on Apr 30, 2021

 PhonicUK added this to Needs triage in AMP Core via automation on Apr 30, 2021

 PhonicUK moved this from Needs triage to High priority in AMP Core on Apr 30, 2021

 PhonicUK moved this from High priority to Closed in AMP Core on Apr 30, 2021

🔍  **PhonicUK** self-assigned this on Apr 30, 2021

**PhonicUK** commented on Apr 30, 2021

Contributor

We are assigning a CVE for this issue. Details to follow.

**PhonicUK** commented on May 4, 2021 • edited

Contributor

This issue was assigned [CVE-2021-31926](#) - The issue was fixed as part of the 2.1.1.2 update.

Assignees

 **PhonicUK**

Labels

core **promoted** security

Projects

 **AMP Core**  
Closed

Milestone

No milestone

Development

No branches or pull requests

2 participants

