



# Chuco Gives a FAQ 2024: 3rd Party Package Egress Rules Guide

Version: 1.0

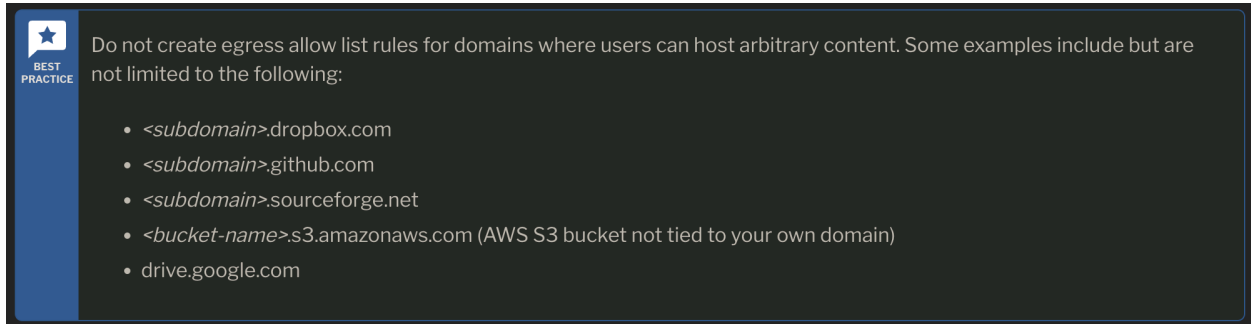
Last Update: Oct 23rd, 2024

# Table of Contents

<b>Tanium Best Practice</b>	<b>3</b>
<b>What About The “Unable to access origin” Error</b>	<b>4</b>
<b>So I Can Just Add github.com?</b>	<b>5</b>
<b>Adding Egress Rules</b>	<b>7</b>

# Tanium Best Practice

Before we dive into egress rules for 3rd party packages in Tanium Deploy, let's review Tanium's best practice guidance.

A screenshot of a Tanium Best Practice notification. It features a dark background with a blue vertical bar on the left containing a star icon and the text "BEST PRACTICE". The main text is white and reads: "Do not create egress allow list rules for domains where users can host arbitrary content. Some examples include but are not limited to the following:". Below this is a bulleted list of domain examples.

- <subdomain>.dropbox.com
- <subdomain>.github.com
- <subdomain>.sourceforge.net
- <bucket-name>.s3.amazonaws.com (AWS S3 bucket not tied to your own domain)
- drive.google.com

*Screenshot from Tanium Resource Center*

[https://help.tanium.com/bundle/ug\\_cloud\\_cloud/page/cloud/configuring\\_network\\_egress\\_allow.html](https://help.tanium.com/bundle/ug_cloud_cloud/page/cloud/configuring_network_egress_allow.html)

*Accessed on 10/23/2024*

# What About The “Unable to access origin” Error

You may have seen this error in Tanium Deploy for software packages with files that point to GitHub.

Software Package Files

HandBrake-1.8.2-x86\_64-Win\_GUI.exe

Unable to access origin "github.com." Use a local file instead.

Origin:

Size:

Sha-256:

https://github.com/HandBrake/HandBrake/releases/download/1.8.2/HandBrake-1.8.2-x86\_64-Win\_GUI.exe

22.68 MB (23,779,832 bytes)

e4c3c965ed05492f73fa261d2e2560ed9f0506474956eefab176c44ee709a1ab

I wouldn't blame you for thinking that this is a clear error message indicating that Tanium Deploy is making an attempt to access the file but failing. It is not. If we take a look at the software package audit log we can see that the file has been successfully cached.

B	D	E	F	Q	R
Software Package ID	Product Name	Product Vendor	Product Version	Files	All Files Cached on Tanium Server
12060	HandBrake	HandBrake	1.8.2	<pre>[{"name": "HandBrake-1.8.2-x86_64-Win_GUI.exe", "type": "remote-file", "location": "https://github.com/HandBrake/HandBrake/releases/download/1.8.2/HandBrake-1.8.2-x86_64-Win_GUI.exe", "sha256": "e4c3c965ed05492f73fa261d2e2560ed9f0506474956eefab176c44ee709a1ab", "size": 23779832, "uncompressedSize": 23779832, "isDownloadedDirectlyByTaniumServer": true}]</pre>	TRUE

So what is this error message really telling us? This error message is hard coded in the Tanium Console UI for certain sites. No attempt is made to actually contact the site, and it will not disappear if the site is actually accessible. Rather than checking the software package audit log, an easy breadcrumb to check is whether the **Deploy** button is live.

# So I Can Just Add github.com?

Not quite. Here are some examples.

## HandBrake

Let's take the HandBrake URL from the screenshot above and plug it into the redirect-checker at: <https://www.whatsmydns.net/redirect-checker>

Code	Description	Visit
302	Found	<a href="#">Visit</a>
200	OK	<a href="#">Visit</a>

It turns out that github.com is not our final destination. We would need to create egress rules for both **github.com** and **objects.githubusercontent.com**.

Let's look at the Igor Pavlov 7-Zip (x64) package from the Tanium Software Deployment Gallery. At first glance this looks like we shouldn't have any issues accessing the file.

If we check that url, we find that the msi is in fact stored on GitHub as well.



# Adding Egress Rules

This is the part where I tell you that Chuco is not responsible for any damages, losses, or other unfavorable outcomes that may occur as a result of following the instructions provided in this guide.

1. Navigate to your Tanium CMP (Cloud Management Portal):  
[https://portal.{instance\\_name}.cloud.tanium.com/](https://portal.{instance_name}.cloud.tanium.com/)
2. Login as a CMP Administrator
3. Follow the instructions in Tanium's documentation to add the urls based on the findings from <https://www.whatsmydns.net/redirect-checker>.

**Tanium Documentation:**

[https://help.tanium.com/bundle/ug\\_cloud\\_cloud/page/cloud/configuring\\_network\\_egress\\_allow.html#configure](https://help.tanium.com/bundle/ug_cloud_cloud/page/cloud/configuring_network_egress_allow.html#configure)