Website Allowlisting

Allowlist phishing websites used for phishing simulations.

- Phishing Website Allowlisting Introduction
- Allowlist Phishing Websites in Microsoft Defender for Endpoint

Phishing Website Allowlisting Introduction

GrintOps invests significant effort into ensuring our phishing websites work without issue. However, depending on the security tools in use, specific issues may arise when attempting to use our phishing websites for simulated phishing purposes.

In the list below, we outline some of the security solutions that may be in-use and whether any allowlisting is needed:

- Google Safe Browsing: **No action required**
- Microsoft Smart Screen: **No action required**
- Microsoft Defender for Endpoint (Web Protection): **Allowlisting required**
- McAfee/Trellix Web Control: **No action required**
- Palo Alto Networks PAN-OS And Prisma Access: **Allowlisting required**
- Sophos Web Protection: **Allowlisting required**
- Cisco Umbrella: **Allowlisting required**
- Fortinet FortiGate: **Allowlisting required**
- VIPRE Endpoint Security: **Allowlisting recommended**

If you're using a web filtering solution outside those listed above, and you're experiencing issues, please **contact the GrintOps team**.

Allowlist Phishing Websites in Microsoft Defender for Endpoint

If your organization uses Microsoft Defender for Endpoint, Microsoft Defender XDR, or other **Microsoft Web Protection** products, your employees may experience issues with loading our simulated phishing websites.

Either a red blocked screen, or a little pop-up from Windows Defender may when attempting to load our simulated phishing websites.

Windows Defender Blocked Popup

Microsoft SmartScreen Blocked Screen

mdefender-red.png

The reason access is blocked is due to the category Microsoft has marked these domains under. To allowlist GrintOps Phishing websites, please follow the below guide.

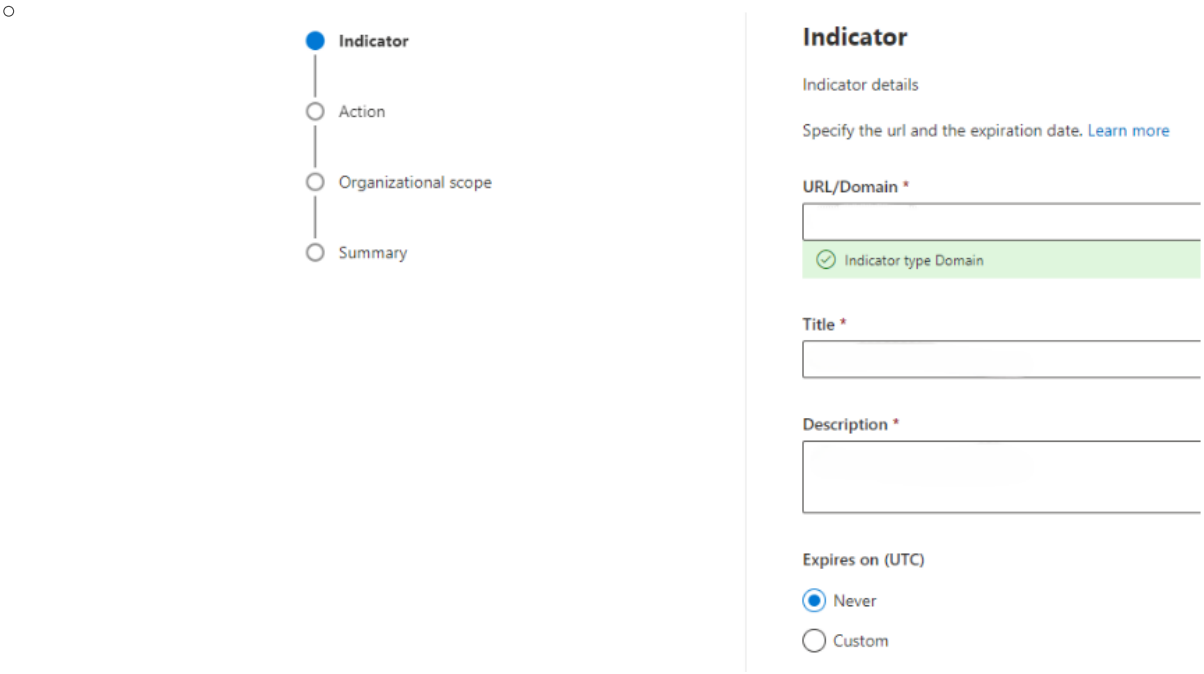
Allowlisting GrintOps Phishing Websites

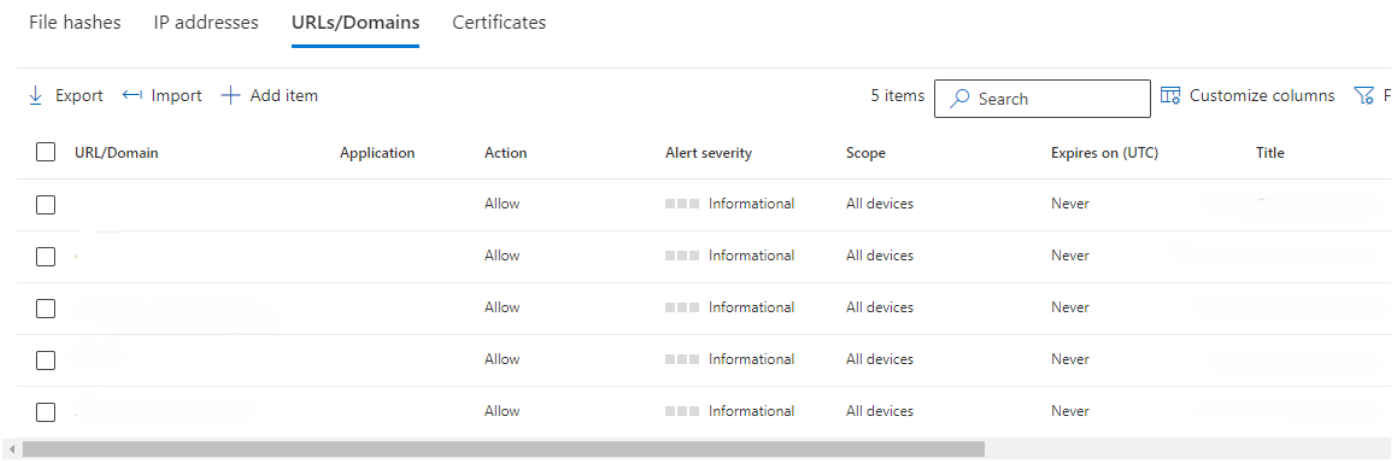
It's possible to override the blocked category in web content filtering to allow a single site by creating a custom indicator policy. The custom indicator policy will supersede the web content filtering policy when it's applied to the device group in question.

To define a custom indicator, follow these steps:

1. In the Microsoft Defender portal, go to Settings > Endpoints > Indicators > URL/Domain > Add Item. (Or click here - https://security.microsoft.com/securitysettings/endpoints/custom_ti_indicators?childviewid=url)

2. **The following are examples of GrintOps phishing website domains to be added under the "Manage URLs to Not Rewrite" section.** One-by-one, enter the following GrintOps phishing website domains with an expiration of your choosing and ensuring the "Allow" action is specified for all devices in your organization:





All done! It takes time for Microsoft to propogate these changes so please wait 1-2 hours for this policy to take effect.