SAML Bypass for Umbrella SWG is Now Available

Contents

Introduction

This document describes the availability of an SAML Bypass for the Umbrella secure web gateway (SWG).

Overview

It is now possible to bypass the SAML user identity challenge by domain or IP address.

Using SAML to obtain a user identity can sometimes cause incompatibilities with certain types of web request. For example, non-browser applications or IoT (Internet of Things) device traffic might not be able to respond correctly to the SAML identity challenge. When the user identity cannot be obtained the request is blocked. If the reason for the failure to respond correctly to a SAML challenge is known to be an incompatibility issue, a SAML bypass can be added to prevent the SAML challenge in future.

Bypassing SAML for a destination means that the user identity is not available to match against user-based polices. Other identity types, such as Network or Tunnel, are used to match the web policy and the request allowed or blocked based on the policy outcome.

A new destination list type called 'SAML Bypass' is now available. The destination list can be added to a Ruleset by editing the SAML setting.

For more information on configuring a SAML bypass please refer to the Umbrella documentation -

1. Add a SAML Bypass Destination List- https://docs.umbrella.com/umbrella-user-guide/docs/add-a-saml-bypass-destination-list
2. Add a Ruleset to the Web Policy-https://docs.umbrella.com/umbrella-user-guide/docs/add-a-rules-based-policy