Troubleshoot "Access Not Allowed" Error in SAML Group

Contents

Introduction

This document describes how to troubleshoot the "Access Not Allowed" error when selecting a SAML group or user as an identity.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Problem

When the web traffic is sent through the tunnel, it only gets redirected to SAML IdP if the tunnel is selected as the identity. If only the SAML group or user is selected as the identity, it does not redirect to IdP and, therefore, gets "Access Not Allowed" as it is not authenticated.

Solution

For SAML authentication to be initiated, a policy must exist for the tunnel identity (or the network identity). And above this policy, a policy can be created based on SAML user/group identity. SAML association is currently based on Tunnel and Network.