"HTTP Status 401 - Authentication Failed: Error validating SAML Message" when You Use SSO

Contents

Introduction

This document describes an issue where you receive an "HTTP Status 401" error message after a period of inactivity when you use Single Sign-On (SSO).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- SSO
- Active Directory Federation Service (AD FS)
- CloudCenter

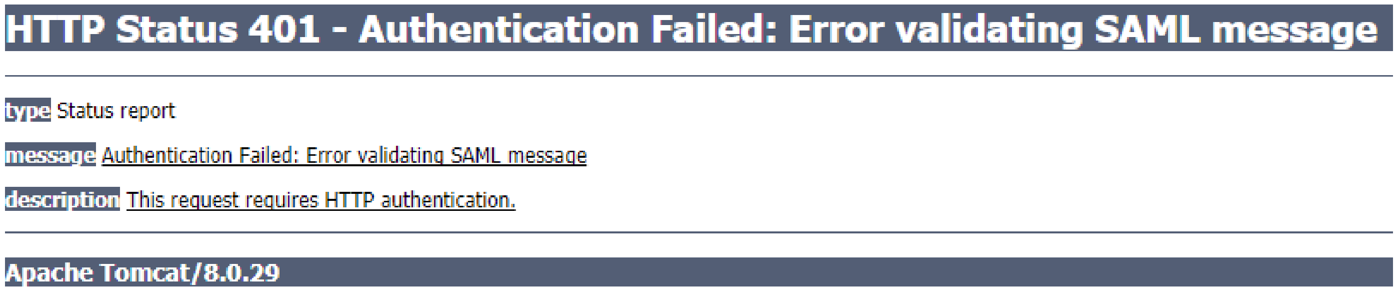
Components Used

This document is not restricted to specific software or hardware versions.

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, make sure that you understand the potential impact of any command.

Problem

When you use SSO, you can receive a "401" error after a period of inactivity, instead of a prompt to log in again as shown in the image.



HTTP Status 401 - Authentication Failed: Error validating SAML message

type Status report

message Authentication Failed: Error validating SAML message

description This request requires HTTP authentication.

Apache Tomcat/8.0.29

The only way for you to be able to log in again is to close the entire web browser and reopen it.

Solution

This is caused by a mismatch in the timeout values between CloudCenter and the SSO server.

An enhancement allows the ForceAuthn Parameters support, which can allow a mismatch between the two values and CloudCenter to log out gracefully. This enhancement can be tracked here https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

The only workaround is to remove the mismatch. There are three locations where the timeout values need to match. The first two are on the CCM itself.

1. Navigate to **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Modify the **<session-timeout>time_In_Minutes</session-timeout>** to reflect the timeout desired in minutes.
3. Navigate to **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Modify the **saml.maxAuthenticationAge.seconds=timeout_in_seconds** to reflect the timeout desired in seconds.

The third is on the SSO server and the location can vary which depends on what type of SSO server is running. The web SSO lifetime value must match the two values configured on CloudCenter.

Once all three match, when the timeout has occurred, you are dropped back to the log in screen before allowed to view the page.