Troubleshoot SAML Assertion Expired SSO Configured with ADFS IdP

Contents

Introduction

This document describes the troubleshooting SSO error "SAML Assertion Expired" while signed in to Cisco Webex App/ Cisco Webex Control Hub.

Prerequisites

Requirement

Cisco recommends that you have knowledge of these topics:

- Single Sign on Configuration
- Webex Control Hub
- ADFS Server and Powershell

Components Used

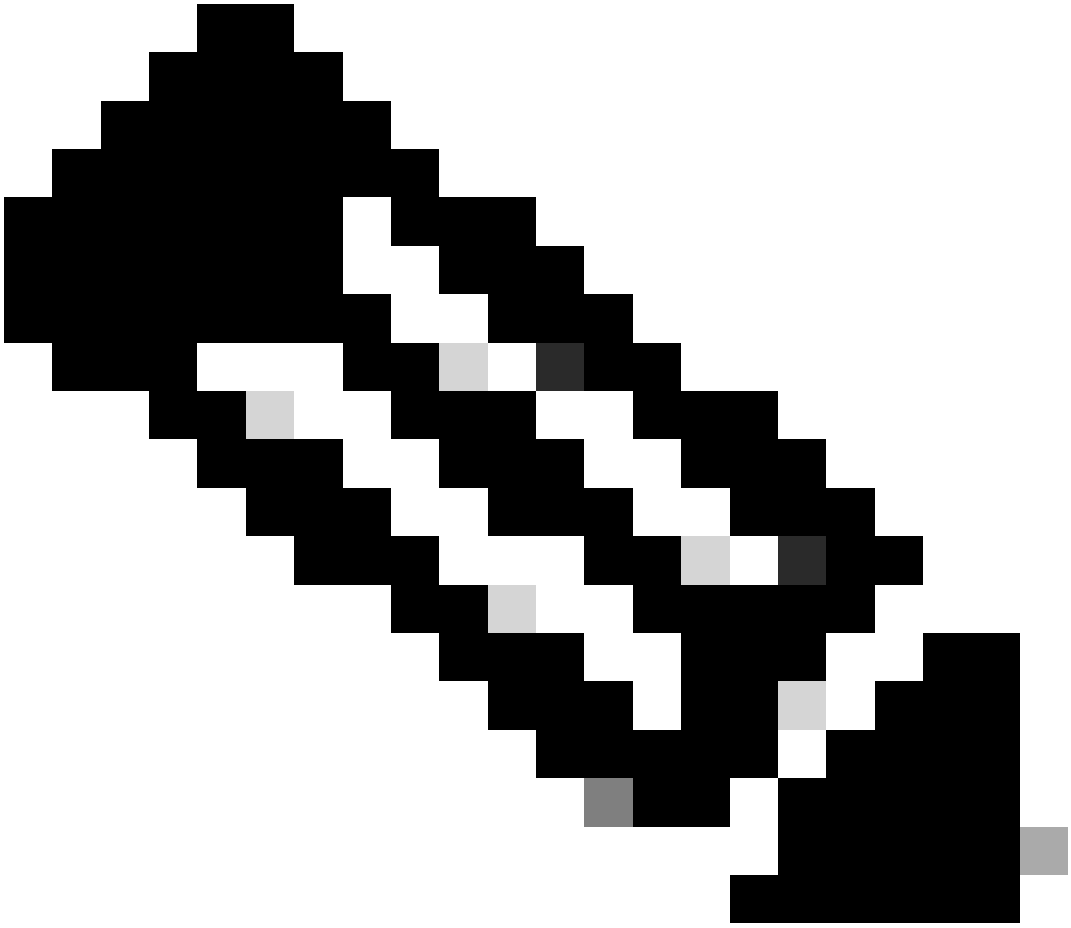
The information in this document is based on these software and hardware versions:

- Windows ADFS server 2022
- Webex Control Hub

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.

Background

This document describes the troubleshooting Single Sign-On (SSO) "SAML Assertion Expired" error while signed in to Cisco Webex App/ Cisco Webex Control Hub which presentes itself after entering the email ID, and completing the SSO flow.



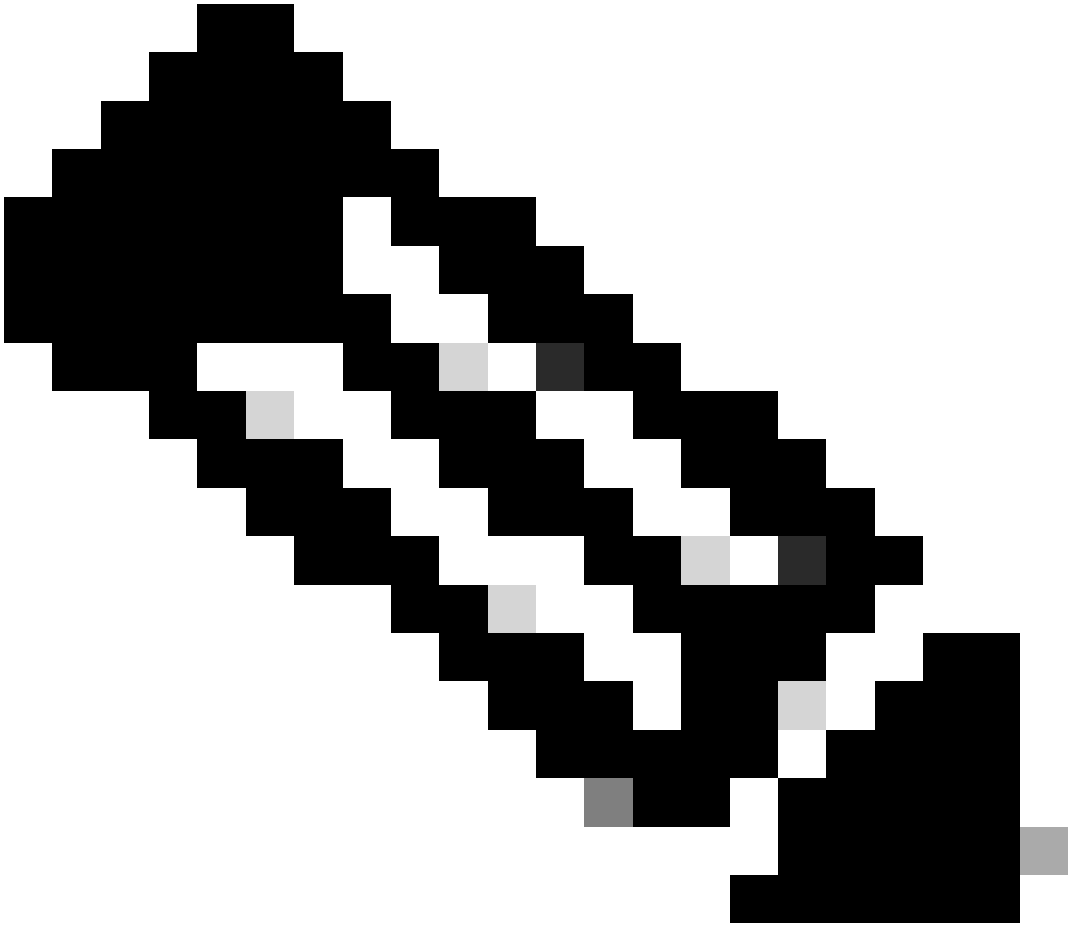
Note: This issue appears mostly on ADFS Server. This document is specific to ADFS IdP only.

Troubleshooting Steps

1. Ensure you are able to log in to ADFS Server using the admin credentials.
2. Check for the error message presented in the login attempt. Ideally, this is a simple fix and one can go through direct troubleshooting of the issue looking at the error message itself.
3. The "SAML Assertion Expired" error message only occurs when the ADFS server time does not match the local machine time. This requires a command to fix the time difference. However, you can review the HAR logs from the local machine and one can see the difference in the HAR response.

Logs Analysis

You can check for login time and before/after time in the HAR logs:



Note: The assertion time must fall between "Not before: Apr 07 2025 09:00:37" and the "Not After: Apr 07 2025 10:00:37 time provided in the SAML" response.

```
Not Before: Apr 07 2025 09:00:37
Not After: Apr 07 2025 10:00:37
Assertion Time: Apr 07 2025 09:00:07
```

Root Cause

Assertion time: Apr 07 2025 09:00:07 did not fall in the range of *not* before and *not* after provided in the SAML response.

Solution

Run this command on the ADFS Server PowerShell to resolve the issue:

Set-ADFSRelyingPartyTrust -TargetIdentifier "SP Entity ID" -NotBeforeSkew 3

This command can be different for different organizations. The best way to get this command is by using the SP (Webex) entity ID from the SP metadata for your org in place of the URL in the command.

SP Entity ID must be in this format: https://idbroker-b-us.webex.com/OrgID.