Troubleshoot SNA Manager SSO Authentication Failure with Azure Entra ID

Contents

Issue

Users experienced SSO authentication failures when attempting to log into SNA Manager after integrating with Azure Entra ID as the Identity Provider (IdP) for SAML authentication. The specific error message displayed was:

"The authentication service was unable to fulfill your request. If this problem persists, contact your administrator."

During the setup process, after importing the SP (Service Provider) metadata file, the SNA Manager FQDN automatically changed from the original SNA Manager URL to include "/fedlet", which contributed to the authentication setup failure. The system audit logs confirmed authentication failures with "Unknown User" errors, indicating that the SNA Manager was not recognizing the usernames being transmitted in the SAML response from Azure.

Environment

- Cisco Secure Network Analytics (SNA) Manager version 7.6.0
- Microsoft Azure Entra ID configured as SAML Identity Provider

Resolution

The resolution involved correcting the SAML NameID attribute configuration in both Azure Entra ID and the SNA Manager to ensure proper username format matching.

Step 1: Perform SAML Trace Analysis

Use browser developer tools to perform a SAML trace and inspect the IdP response from Azure to identify the NameID format being transmitted. The trace revealed that Azure was sending the full User Principal Name (UPN) in the NameID attribute:

<#root>

<Subject><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" SPNameQualifier="https:/

username@example.com<

/NameID>

Step 2: Review SNA Manager Audit Logs

Check the SNA Manager audit logs to confirm authentication failures correlating with the malformed NameID:

Aug 3 06:53:36 device AuditLogger[1480861]: AuditLogger: osaxsd/1480861,4003,2026-08-03T06:53:36TZD+000

Step 3: Modify Azure SAML NameID Configuration

In the Azure Entra ID SAML configuration, change the NameID attribute from the default User Principal Name to use the **"On-premises SAM account name"**. This ensures that the NameID contains only the username without the domain suffix (username@example.com becomes username).

Step 4: Update SNA Manager SAML ID Configuration

Navigate to the SNA Manager user management page and update the SAML ID value to match the corrected NameID format that is transmitted by Azure after the configuration change.

Step 5: Verify SSO Authentication

Test the SSO authentication by attempting to log in through the SAML workflow. The user now successfully authenticates without receiving the previous error message.

Cause

The authentication failure was caused by a mismatch between the NameID format sent by Azure Entra ID and the username format expected by the SNA Manager. Azure was configured to send the User Principal Name (UPN) in the format "username@example.com" in the SAML NameID attribute, while the SNA Manager expected only the username portion without the domain suffix. This format discrepancy resulted in the SNA Manager treating the incoming authentication requests as coming from unrecognized users, leading to "Unknown User" authentication failures.

Related Content

- Configure SNA Manager for Microsoft Azure SAML Integration
- Cisco Technical Support & Downloads