Tenable FedRAMP SAML/SSO Configuration Guidance

Setup, Common Errors, and Troubleshooting

Last Revised: August 14, 2023

Table of Contents

Initial Tenable Vulnerability Management FedRAMP SAML Configuration

Initial Pre-sales SAML Setup

The initial pre-sales SAML setup for FedRAMP customers includes the following steps:

1. The Tenable customer creates an XML, IDP initiated SAML metadata object (for example, IDP.xml) and sends it to their Tenable representative.

   > **Note:** The FedRAMP container Tenable includes one pre-defined Administrator user, which is based on the NameID parameter (an email address in user@domain format) specified in the SAML metadata object. This user is the only person who can log into the container upon initial creation. If the customer wants to allow additional domains to log in to the container upon creation, they must specify these additional domains ahead of time.

2. Tenable extracts the certificate from this file and creates the FedRAMP container with a custom URL.
3. Tenable sends the custom URL back to the customer.
4. The customer can then finish their SAML setup using the URL.

SAML Setup for Manual Configuration of Customer SAML

Manual Configuration of Customer SAML requires the following:

- Audience URI (SP Entity ID): NessusCloud (or a custom ID, only if specified by Tenable.) If the customer requires more than one FedRAMP container, Tenable requires different SP Entity IDs for each container.
- Application Username: A mapped email address, or an address in user@domain format.

  > **Note:** This must match the NameID parameter.

- NameID: The address to use for the primary Administrator user in user@domain.xxx or email address format.
- Login URL: A custom URL provided by Tenable after provisioning the FedRAMP container.
- A Certificate within the SAML metadata object that matches the data originally sent to Tenable.

Note: We do not support the use of multiple certificates and only extract the first certificate from the metadata object. If the object includes multiple certificates, the customer must specify which certificate to use if it is not the first one listed.

After the customer successfully logs in using the primary Administrator login, they can create other user accounts within their FedRAMP container.

Common IDP Misconfigurations

Tenable Vulnerability Management FedRAMP SAML/SSO is IDP initiated. As such, the most common errors are due to IDP misconfiguration. Often, the issue is a minor error such as a typo on an Entity ID. Other times, errors can be more complicated, like the misconfiguration of a transform rule preventing successful SAML authentication.

> **Note:** FedRAMP Splunk includes an error tracker that provides helpful context for errors. If the initial troubleshooting in this guide does not fix the error, contact a FedRAMP Splunk support representative. Tenable Support can also examine errors to provide further insight for troubleshooting efforts.

The following are some of the most common IDP misconfiguration errors:

- `“incorrectly signed, or missing field”`
    - This error typically indicates something is wrong with the certificate/s in the idp.xml file. Since Tenable Vulnerability Management currently only uses the top certificate in the file, this error could indicate your XML certificates are out of order. Identify the primary certificate with the customer. Usually, you can mitigate this error by manually selecting the correct certificate within Tenable Vulnerability Management.
    - Alternatively, the certificate may be expired. Inspect the file and make sure it does not include any expired certificates.
- `“This Username does not exist.”`
    - Verify the following:
        a. The NameID
        b. The transform claim rule for the incoming claim is set to Email
        c. The outgoing claim type is configured to NameID
    - The signature may be showing as not validated in Splunk. Work with Tenable Support to use the correct certificate.
- `“{"error":"SAML login attempt failed."}”`
    - The container has likely expired. Contact Tenable Support to review the Splunk logs for supporting information.

- If the error includes the following warning:

  ```
  WARN [2022-xxxxx 13:38:06,520][dw-38 - POST /saml/login/xxxxxxxxxxx] [X-Request-Uuid=xxxxxxxxxxxx][c.t.c.w.m.manager.UserManager] id-269: user-locate: Could not find a user: CacheLoader returned null for key (usernamexxxxxxxx)
  ```

  Their IDP.xml file is passing what appears to be just {lastname}{firstname_firsttwo} instead of {lastname}{firstname_firsttwo}@{domain}. The customer must adjust their claim and/or transform rules accordingly.

- “`{"error":"SAML login attempt failed - the SAML IdP configuration was found, but no username could be extracted from the SAML message (could be incorrectly signed, or missing a field)."}`”

  - The following error in FedRAMP Splunk indicates SAML was not configured when the user attempted to log in with their username and password.

    ```
    User[username=xxxxxxx@domain.com] is not permitted to authenticate with a password
    ```

- “`SAML validation failed against container xxxxxx-xxxxxxxxxx- org.opensaml.xml.validation. ValidationException: Assertion audience does not include issuer`”

  - The problem is with the customer SAML assertion configuration. In the IDP.xml file, check Audience URI or SP Entity ID parameters. Additionally, verify the NameID parameter is in the correct format.

- Customers that have multiple Tenable Vulnerability Management FedRAMP containers or a customer that has a commercial Tenable Vulnerability Management container already configured for use with SAML could also encounter an error where the IDP is unable to support multiple instances of the same Entity ID. If the parameter is listed as anything other than NessusCloud, Tenable Support must be notified during the initial request of the FedRAMP container; they can provide sp.xml file to send back to the customer with the appropriate information.

Troubleshoot Okta IDP Configuration

Ensure the Okta IDP information includes the following information:

- SSO URL = The URL provided by Tenable (for example, https://fed-cloud.tenable.com/saml/login/xxxxxxxxxxxxxxxxxxxx)
- Recipient URL = The recipient URL provided by Tenable (as listed above)
- Destination URL = The destination URL provided by Tenable (as listed above)
- Audience Restriction (SP Entity ID) = set to NessusCloud
- Check if the NameID parameter is set to Unspecified. Sometimes this works initially because their default was "user.email", but in some cases may need to be reconfigured:
    - Choose the NameID format and the application username sent to your application in the SAML response (for example EmailAddress and Email)
    - In the Attribute Statements (optional) section, type the SAML attributes to be shared with your application. For example:
        - Name (in SAML application) Value (in Okta profile)
        - FirstName user.firstName
        - LastName user.lastName
        - Email user.email (edited)

For more information on Okta IDP configuration, see the following resources:

- Okta Developer Portal
- Create SAML App Integrations
- Build a Single Sign-On Integration
- Create a SAML Integration in Okta