USING SAML FOR AUTHENTICATION

This is only valid for the MSV (on-prem) version of Security Validation.

Most SAML products require information about the target application, such as the URLs for Secure SSO (SSSO), Recipient, and Destination. When setting up SAML with the Director, use the following information:

- Single Sign On URL: `https://directorIP/users/saml/auth`
- Recipient URL: `https://directorIP/users/saml/auth`
- Destination URL: `https://directorIP/users/saml/auth`
- Audience Restriction: `https://directorIP/users/saml/metadata`

The SAML Authentication form in the platform does not change for the different SAML products. However, where you find the required information in the SAML product is unique, so use the product's documentation to identify the required information. We will continue to update this section with additional SAML products. If your product is not listed, you can still use the available process as a basis for your setup.

Authentication integrations are only for authentication; user permissions still need to be defined in the Validation Platform.

Enable SAML authentication with Okta

1. Go to **Settings > User Settings**. The User Settings page opens.
2. Select **Authentication**.
3. Enter the fully qualified domain name of your Director in the **Director Hostname for SAML URLs** field, if you want to use the FQDN instead of the IP address.

   FQDNs must comply with RFC 1123, a standard that defines the requirements for FQDNs on the internet. This standard specifies that FQDNs can only contain the following:
   - Letters (A-Z, a-z)
   - Digits (0-9)
   - Hyphens (-)

   Underscores are not permitted.

   For more information, see **RFC 1123: Requirements for Internet Hosts (https://www.rfc-editor.org/rfc/rfc1123.html)**.

4. Select **SAML**.
5. Define the authentication fields, which are provided by your identity provider and are unique per product.
   a. Enter the **SAML - Name Identifier Format**.
      Get this from the metadata file `<md:NameIDFormat>`.
   b. Enter the **SAML - AuthN Context**.
   c. Enter the **SAML - idP SSO URL (Login)**.
      Get this from the metadata file in the Location field
      `<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=""/>`.
   d. Enter the **SAML - IdP SLO URL(Logout)**.
      This is the same as the Login information.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

   e. Enter the **SAML - IdP Certificate**.
      Get this from the metadata file: `<ds:X509Certificate>`.
   f. Enter the **SAML - Attribute Map**.
      This field may autopopulate after defining the other authentication fields.

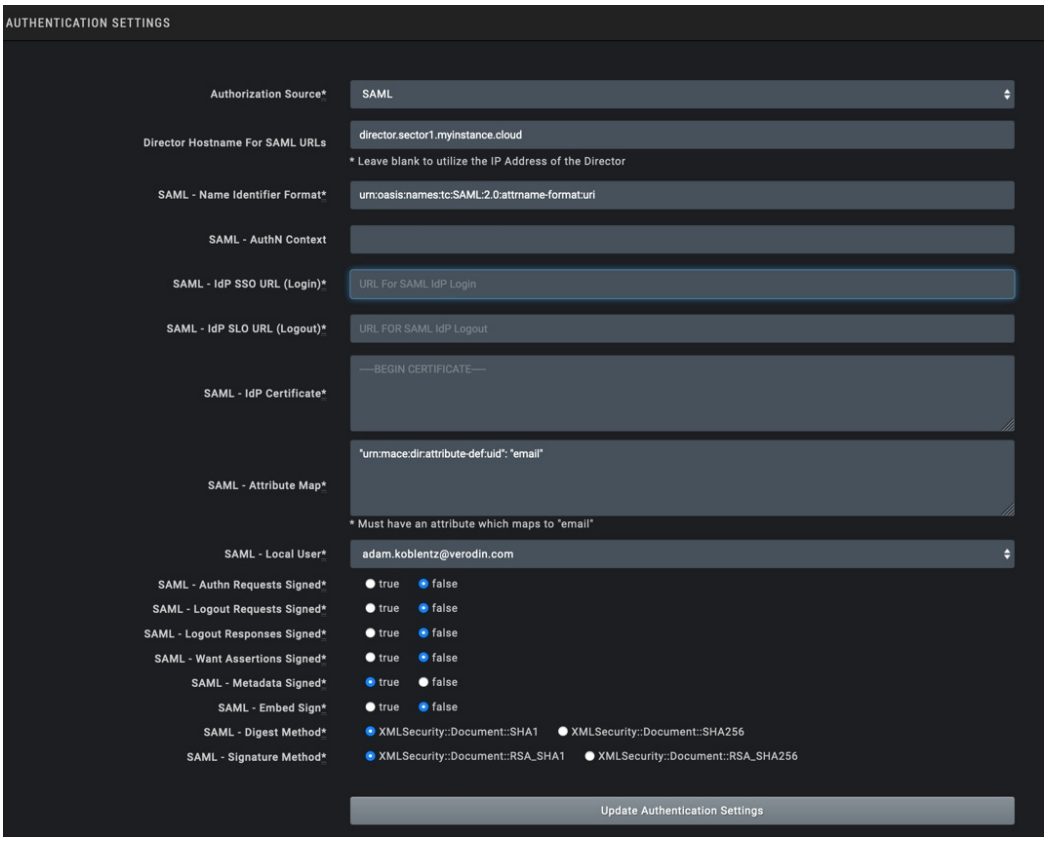
6. Select the **Local User**.
   This is the Admin user in the Director that can sign into the Director without using SSO.
7. Based on your Authentication and security requirements, set the following to either true or false:

   These features need to be supported by the identity provider (SSO service).

   a. **SAML - Authn Requests Signed**.
   b. Enter the **SAML - Logout Requests Signed**.
   c. Enter the **SAML - Logout Responses Signed**.
   d. Enter the **SAML - Want Assertions Signed**.
   e. Enter the **SAML - Metadata Signed**.

8. Enter the **SAML -Digest Method**
   This is the hash of the entire message in a SAML assertion and is dependent on the implementation. The Validation Platform supports SHA1 and SHA256.
9. Enter the **Signature Method**.
   This is signature of the message from the identity provider and is dependent on the implementation of the SSO solution.
10. Click **Update Authentication Settings**.
    The platform is ready for SSO with Okta.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.



SAML with Okta Authentication setup screen

Update SP certificate

By default, the Service Provider uses a self-signed certificate. If you want to use a custom signed certificate (such as the same SSL certificate configured for your Director's web server) to help ensure proper SAML authentication, follow these steps:

1. Go to **Settings > User Settings**. The User Settings page opens.
2. Select **Authentication**.
3. From the SAML settings page, click **Update Verodin SAML SP Certificate Update Director SAML SP Certificate**.
4. In the fields provided, paste your custom **Certificate** and **Private Key**.

   > If you want to use the same custom certificate configured for your Director's web server, you can copy the certificate and key from `/etc/httpd/ssl/apache.crt` and `/etc/httpd/ssl/apache.key` on your Director.

5. Click **Save**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.