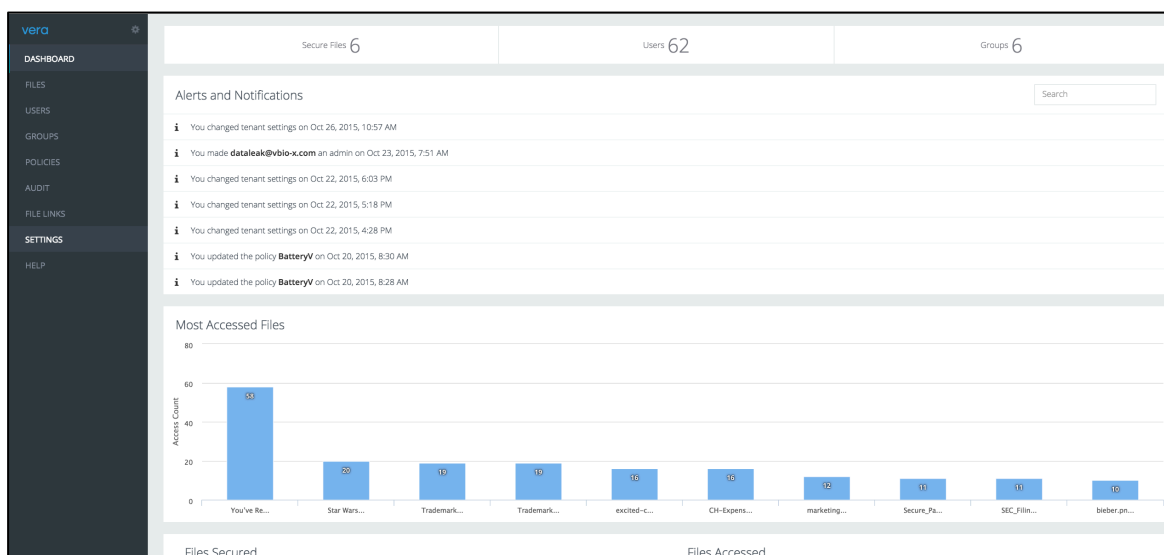


Vera for Okta – How to set up the integration

How to configure SAML 2.0 for Vera

Case 1: For Okta users not using Group Push

1. Copy the following **IDP Metadata** and save as a .xml file:
[The Okta Dashboard will generate this variable]¹
2. Log in to your Vera account.
3. Navigate to the **Settings** page:



4. On the **Settings** page, navigate to the **Authentication** tab, and scroll to **Internal Authentication** section.
5. Enter the following values into the corresponding fields in Vera (see screen capture at end of step for reference):

¹ Okta team: please use box in current set up instructions.

Vera for Okta – How to set up the integration

- Select the **Authentication type: SAML**
- **SAML Metadata:** Click **Choose file**, and upload the .xml file you saved in step 1.
Copy the following into the **Login URL** field: [The Okta Dashboard will generate this variable]²
Copy the following into the **Logout URL**: [The Okta Dashboard will generate this variable]³
- **Email attribute:** Enter **user.userName** (enter as is)
- **Groups attribute:** Leave the default values.
- **Internal Domains and Users:** Enter the domain name of the username that will be using SAML to access the account. For example, if the username is johndoe@mycompany.com, enter mycompany.com in this field. Or, you can also manually enter the usernames of all the users who will be using SAML under the **Users** section.

The screenshot shows the 'Internal Authentication' configuration page in the Vera web interface. The left sidebar contains navigation links: SETTINGS, GENERAL, RULES, ROLES, SHARES, AUTHENTICATION (selected), SAML, and CONNECTORS. The main content area is titled 'Internal Authentication' and includes the following sections:

- Authentication Type:** A dropdown menu set to 'SAML'.
- SAML Metadata:** A section with a 'Choose file' button and a note: 'You have uploaded a SAML metadata file'.
- Login URL:** A text field containing 'https://dev-76030555.oktapreview.com/opa/verafx/saml/cheatkeyid/1778000000'. Below it, a note says 'The login URL from your SAML provider'.
- Logout URL:** A text field containing 'https://dev-734869-oktapreview.com'. Below it, a note says 'The logout URL from your SAML provider'.
- Email Attribute:** A text field containing 'user.userName'.
- Groups Attribute:** A text field containing 'groups'.
- Auto-Create SAML Groups As Local Groups:** A checkbox that is checked.
- Max Authentication Session Timeout:** A text field containing '1440' with a note '(in minutes)'.
- Internal Domains:** A section with a dropdown menu showing 'vera.com', 'verafx.com', and 'vera.com' (selected). Below it, a note says '(please refer to the documentation)'.
- Internal Users:** A section with a dropdown menu showing 'Select or enter one or more users'.

² Okta team: please use box in current set up instructions.

³ Okta team: please use box in current set up instructions.

Vera for Okta – How to set up the integration

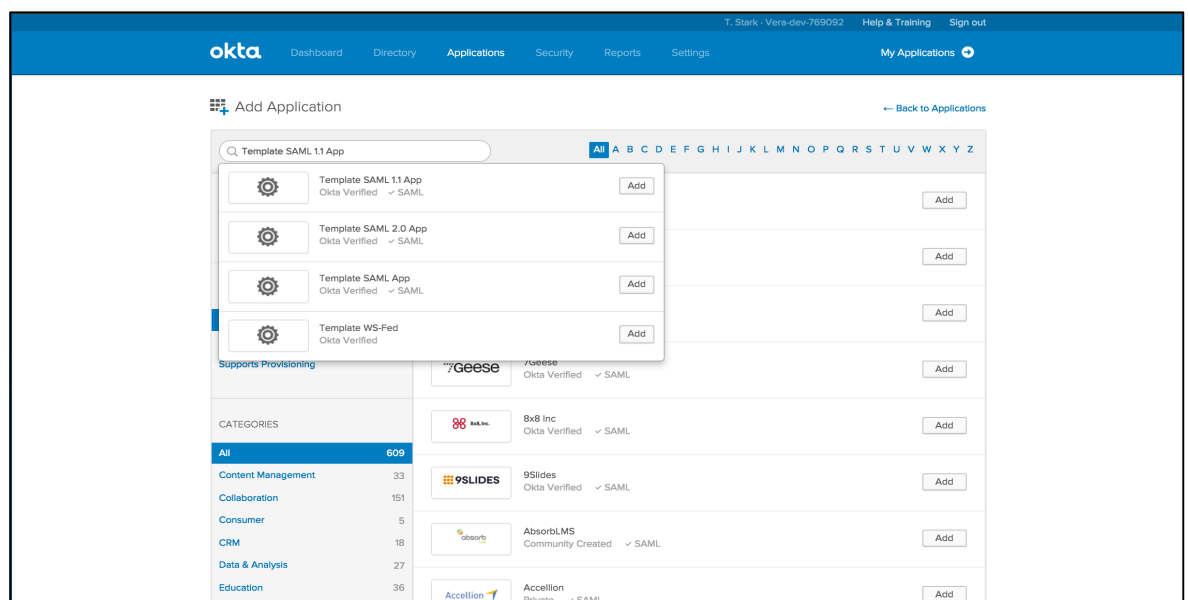
6. Click **Save** in the top right corner.

The screenshot shows the 'Authentication Settings' page in the Vera application. The left sidebar contains navigation links: SETTINGS, GENERAL, RULES, RULES, SHARES, AUTHENTICATION (highlighted), SAML, and CONNECTORS. The main content area is divided into two sections: 'Default Authentication' and 'Internal Authentication'. The 'Default Authentication' section has fields for 'Authentication Type' (set to Email), 'Domains Allowed to Authenticate' (with a placeholder 'Enter one or more domains'), and 'Users Allowed to Authenticate' (with a placeholder 'Select or enter one or more users'). The 'Internal Authentication' section has fields for 'Authentication Type' (set to SAML), 'SAML Metadata' (with a placeholder 'Drop a SAML metadata file here, or click to select a file to upload'), 'Login URL' (with a placeholder 'The login URL from your SAML provider'), 'Logout URL' (with a placeholder 'The logout URL from your SAML provider'), 'Email Attribute' (set to user.userName), 'Groups Attribute' (set to Groups), and 'Max Authentication Session Timeout' (set to 1440). A 'Save' button is located in the top right corner.

7. Done.

Case 2: For Okta users using Group Push

1. From the Okta Application Network dashboard, navigate to the **Admin** tab. (Note: you must be the Okta admin to configure Vera.)
2. Select the **Applications** tab and search for **Template SAML 2.0 App**.



Vera for Okta – How to set up the integration


3. Enter the following values to the following fields in the **General Settings** for the new **Template App**. See the screen shots in line for reference.
 - a. **Application Label:** The name that will appear under the app on the Vera home page.
 - b. **Post Back URL:** <https://<yourSubDomain>.vera.com/api/auth/req/verify>
 - Example: <https://acme.vera.com/api/auth/req/verify> where “acme” is the sub domain name.
 - c. **Name ID Format:** **Email Address**
 - d. **Recipient:** <https://<yourSubDomain>.vera.com/api/auth/req/verify>
 - e. **Audience Restriction:** <https://<yourSubDomain>.vera.com/api/auth/req/verify>
 - f. **authnContextClassRef:** **PasswordProtectedTransport**
 - g. **Response:** **Signed**
 - h. **Assertion:** **Signed**
 - i. **Request:** **Uncompressed**
 - j. **Destination:** <https://<yourSubDomain>.vera.com/api/auth/req/verify>

The screenshot displays the 'App Settings' configuration window for a 'Template SAML 2.0 VeraApp'. The window is titled 'Template SAML 2.0 VeraApp' and includes an 'Active' status indicator and a 'View Log' link. The settings are organized into a list of fields with their respective values and descriptions:

- Application label:** Template SAML 2.0 VeraApp. This label displays under the app on your home page.
- Force Authentication:** ☐. Prompt the user for their credentials when a SAML request has the ForceAuthn attribute set to true, even if they are already logged in to Okta. If this box is left unchecked the flag will be ignored.
- Post Back URL:** <https://chobbsstaging.vera.com/api/auth/req/verify>. The Post Back URL for this application.
- Name ID Format:** EmailAddress. Name ID Format.
- Recipient:** <https://chobbsstaging.vera.com/api/auth/req/verify>. Recipient.
- Audience Restriction:** <https://chobbsstaging.vera.com/api/auth/req/verify>. The assertion containing a bearer subject confirmation MUST contain an AudienceRestriction including the service provider's unique identifier as an Audience. Example.
- authnContextClassRef:** PasswordProtectedTransport. Authentication Context. urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport.
- Response:** Signed. Select Signed if the Response is signed.
- Assertion:** Signed. Select Signed if Assertion is signed.

Vera for Okta – How to set up the integration

- k. **Default Relay State:** Leave this field empty.
- l. **Attribute Statements:** Leave this field empty.
- m. **Group Name:** Type in the name groups. As a general rule, if you're in a group, we want to bring
- n. **Group filter:** Enter an expression that will be used to filter groups. For example: **app1.*** includes all groups prefixed with the string **app1**. This field accepts regular expression syntax
- o. **Application Visibility:** Leave unchecked

Request	<div>Compressed </div> <div>Select Compressed if the Request is compressed</div>
Destination	<div><input type="text" value="https://chobbsstaging.vera.com/api/auth/req/verify"/></div> <div>Destination for SAML Response</div>
Default Relay State	<div><input type="text"/></div> <div>Default Relay State is used in IDP initiated Single Sign-On POST If no value is set, a blank RelayState is sent.</div>
Attribute Statements	<div><input type="text"/></div> <div>Default Namespace is urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified Format: FirstName\${user.firstName},LastName\${user.lastName},ManagerName\${user.customField} To include the custom attributes of the user in the format \${user.customField}, make sure that the field 'customField' has been set to the users profiles. To include namespace for the attribute, Format: AttributeName/AttributeValue/AttributeNamespace Can specify the namespace firstName\${user.firstName}urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified,roleENGLurn:oasis:names:tc:SAML:2.0:attrname-format:unspecified</div>
Group Name	<div><input type="text" value="groups"/></div> <div>When this option is set, if a user belongs to any groups in Okta, those groups will be included in the SAML Response Attribute statement. Used in conjunction with Group filter</div>
Group filter	<div><input type="text"/></div> <div>Create an expression that will be used to filter groups. If the Okta group name matches the expression, the group name will be included in the SAML Response Attribute statement Example: app1.* would include all groups prefixed with the string "app1". Uses regular expression syntax</div>
Application visibility	<div><input type="checkbox"/> Do not display application icon to users</div> <div><input type="checkbox"/> Do not display application icon in the Okta Mobile App</div>
<div>Save</div>	

Vera for Okta – How to set up the integration

4. Select **Save**.
5. Assign the application to a user, then click **Done**.
6. Select the **Applications > Sign On** tab then select **View Setup Instructions**. Scroll down to the **Configuration Data** section to retrieve the data you'll need for the next step.
7. Login to your Vera account, and follow the instructions outlined in **Case 1: For groups not using Group Push** above, except use the data in the setup instructions you just opened for the values for Login URL, Logout URL, etc.
8. Done!