## Authentication with Okta and SAML2

Last Modified on 12/30/2024 4:15 pm EST

## PoliteMail User Authentication with SAML2 and Okta

- 1. Open Okta and click the Applications tab, then the Get Started tab, and the 'Create New App' button. The 'Create a New Application Integration' window will appear.
- 2. Select 'Web' from the Platform drop-down menu. Click the SAML 2.0 radio button, then click 'Create'. You will be taken to the application wizard.
- 3. The Application Wizard has three steps: General Settings, Configure SAML, and Feedback.
  - 1. For General Settings:
    - The Application Name should be 'PoliteMail SAML' for easy reference.
    - Check both App visibility options so they are both selected, then click 'Next'.
  - 2. For the Configure SAML step:
    - Single Sign On URL: https://[YourPoliteMailHostname]/ssv3/Saml2/Acs.
    - Use this for Recipient URL and Destination URL: Checked
    - Audience URI (SP Entity ID): https://[YourPoliteMailHostname]
    - Set Name ID format: EmailAddress
    - Application username: Email
    - Update application username on: Create and update
  - 3. Click 'Show Advanced Settings'.
    - Response: Signed
    - Assertion Signature: Signed
    - Signature Algorithm: RSA-SHA256
    - Digest Algorithm: SHA256
    - Assertion Encryption: Unencrypted
    - Enable Single Logout: Unchecked
    - Assertion Inline Hook: None (disabled)
    - Authentication context class: Password
    - Honor Force Authentication: Yes
    - SAML Issuer ID: http://okta.com/\$(org.externalKey)

4. Download the Okta Certificate and place it on the

- PoliteMail server.
- 5. Attribute Statements:

Okta Certificate

Import the Okta certificate to your identity Provider if required.

Ł Download Okta Certificate

Nam		Name Format	Value
http:/	/schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddre	URI Reference	user.email
http:/	/schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	URI Reference	user.firstName
http:/	/schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	URI Reference	user.lastName
	6. Group Attribute Statements:		
	Name N	ame Format	Filter

Name	Name Format	Filter
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role	URI Reference	Starts with PoliteMail

- 7. You will need to create either 4 Directory Groups for PoliteMail: PoliteMailSystemAdministrator, PoliteMailAdministrators, PoliteMailManager, and PoliteMailUser. These names will be mapped on the PoliteMail server.
- 8. You'll now get to the third step, Feedback. Fill out those fields as they apply to your organization, and click on 'Finish' when completed.

After you click 'Finish', you will be redirected to the Settings page.

ack to Applications	
PoliteMail SAML2	
Active View Logs	
neral Sign On Provisioning Import Assignments	
	About
	SAML 2.0 streamlines the end user experse webby not requiring the user to know their credentials. Users cannot edit their indentials when SAML 2.0 is
SIGN ON METHODS The sign-on method determines how a user signs into and manages their credentials for an application. Some sign- on methods require additional configuration in the 3rd party application.	configured for this application. Additional configuration in the 3rd party application may be required to complete the materia unit. Occumplete the
Application username is determined by the user profile mapping. Configure profile mapping	Application Username
® SAML2.0	Choose a format to use as the default username value when assigning the application to users.
Detbult Heildy Stote	If you select None you will be prompted to enter the username manually when assigning an application with password or profile outh provisioning features.
SAML 2.0 is not configured unit you complete the setup instructions	prome pusit provisioning reduires.

Click on 'View Setup Instructions'. This will take you to the Okta configuration page and will display the IDP SSO URL, IDP Issuer (Entity ID), and the X.509 Certificate. Send **all three** of these items to PoliteMail Support.