RSA SecurID Access SAML Configuration for ThousandEyes

Last Modified: Feb 21, 2017

ThousandEyes, Inc. is a network monitoring company based in San Francisco, CA. The company produces software that analyzes the performance of local and wide area networks. ThousandEyes is privately held and backed by venture investors including Sequoia Capital, Sutter Hill Ventures, Salesforce, Tenaya Capital and GV**.**

Before You Begin

- Acquire an administrator account for both RSA SecurID Access and ThousandEyes.
- Obtain the ThousandEyes login URL, ACS URL and Service Provider Issuer ID from your ThousandEyes service provider.

The instructions in this guide use the following login url, ACS URL and issuer ID (entity ID) values:

Login URL	*https://app.thousandeyes.com/login*
ACS URL	*https://app.thousandeyes.com/login/sso/acs*
Service Provider Issuer ID	*https://app.thousandeyes.com*

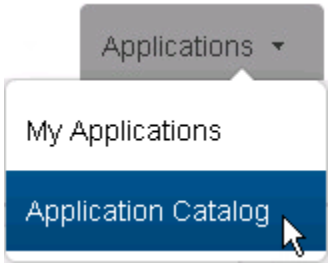
Procedure

1. Add the Application in RSA SecurID Access
2. Configure ThousandEyes to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

1. Log in to the RSA SecurID Access Administration Console, click the **Applications** tab and select *Application Catalog* from the **Application** tab dropdown list.

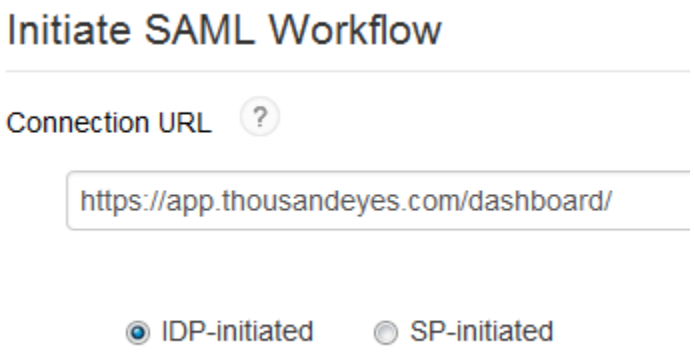


2. Search for *ThousandEyes* in the list of applications and click the **+Add** button.

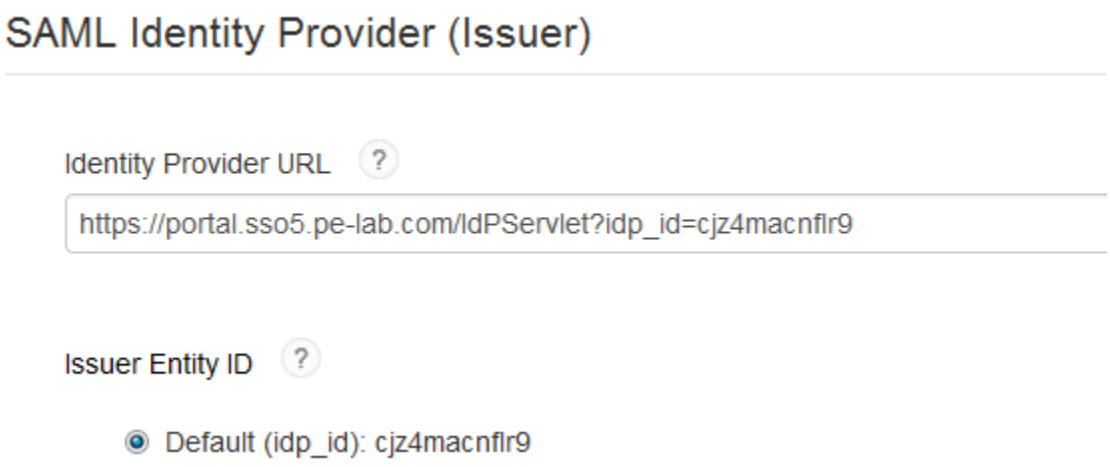
3. Enter a name for the application in the **Name** field on the **Basic Information** page and click the **Next Step** button.
4. Select the **IdP-initiated** radio button in the **Initiate SAML Workflow** section.

Note: The following IdP-initiated configuration works for SP-initiated ThousandEyes connections as well.

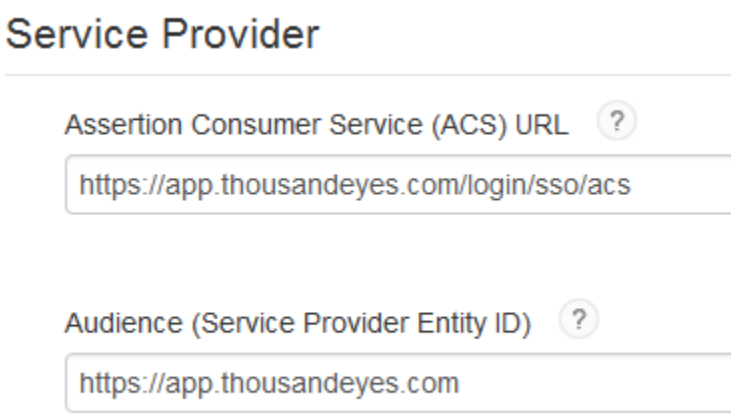
5. Enter the ThousandEyes landing page URL in the **Connection URL** field. Portal users will be redirected to this page when they click the ThousandEyes icon.
   The URL is formatted as follows: https://app.thousandeyes.com/dashboard/



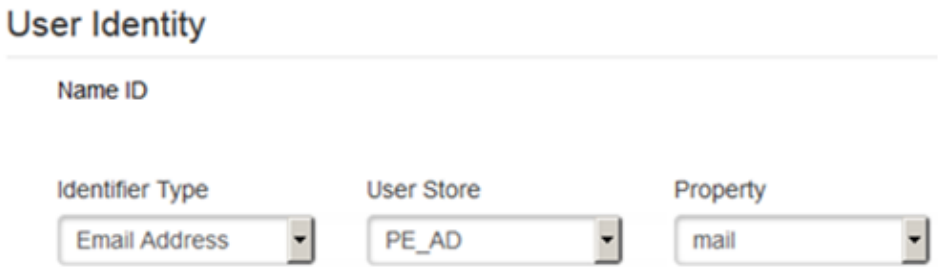
6. Scroll to **SAML Identity Provider (Issuer)** section, copy the value in the **Identity Provider URL** field and paste it into a temporary file. You will need the URL when you configure your ThousandEyes service provider.
7. Copy the value in the **Issuer Entity ID** field and paste it into a temporary file.



8. You must import a private/public key pair to sign and validate SAML assertions. If you don't have one readily available, follow the steps to generate a certificate bundle. Otherwise, continue to step 9.
    a. Click the **Generate Certificate Bundle** button in the **SAML Response Signature** section.
    b. In the **Common Name (CN)** field, enter the hostname of the ThousandEyes service provider's HTTPS server that will be sending authentication requests.
    c. Click the **Generate and Download** button, save the certificate bundle ZIP file to a secure location and extract its contents. The ZIP file will contain a private key, a public certificate and a certificate signing request.
9. Click the **Choose File** button on the left of the **Generate Certificate Bundle** button, locate and select a private key for signing the SAML assertions and click the **Open** button.
10. Click the **Choose File** button underneath the **Generate Certificate Bundle** button, locate and select your public certificate and click the **Open** button.
11. Select the **Include Certificate in Outgoing Assertion** checkbox.
12. Scroll to the **Service Provider** section and enter your ThousandEyes ACS URL in the **Assertion Consumer Service (ACS) URL** field. The URL should be formatted as follows: https://app.thousandeyes.com/login/sso/acs
13. Enter *https://app.thousandeyes.com* in the **Audience (Service Provider Entity ID)** field. This value is case sensitive, and it must match your ThousandEyes SP Issuer ID.

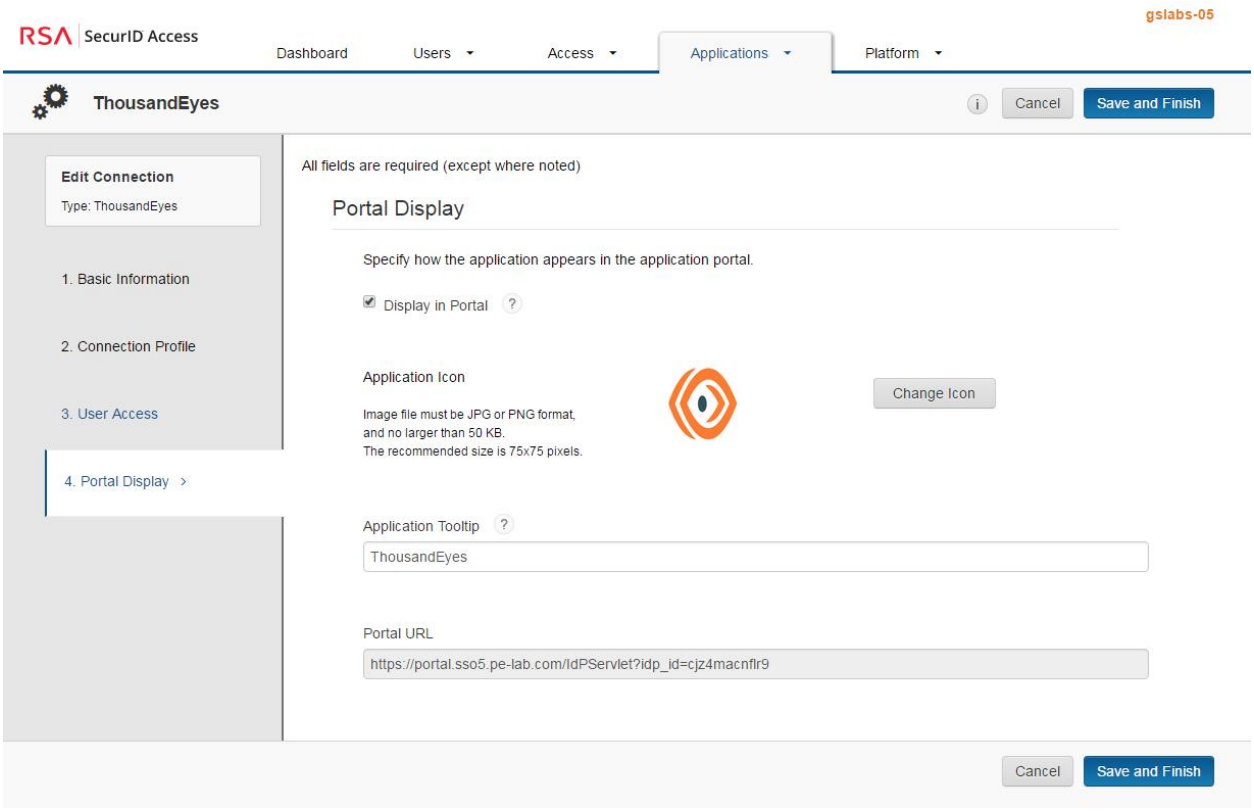


14. Scroll to the **User Identity** section, select *Email Address* from the **Identifier Type** dropdown list and select the name of your user identity source from the **User Store** dropdown list. In this example, user accounts are stored in an identity source named *PE_AD*.
15. Select the identity source's attribute that will be used as the NameID from the **Property** dropdown list. In this example, the identity source's *mail* attribute will be used to uniquely identify a user in SAML assertions.

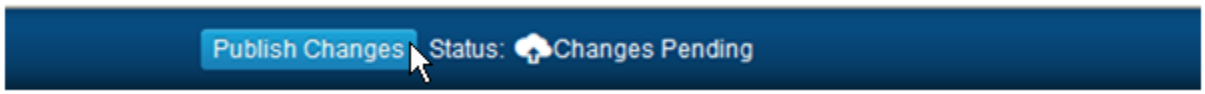


16. Click the **Next Step** button.
17. On the **User Access** page, select the access policy the identity router will use to determine which users can access the ThousandEyes service provider from the portal. If you want to allow access to all users who are signed in to the portal, select the **Allow All Authenticated Users** radio button. Otherwise, select the **Select Custom Policy** radio button and select the policy you want to use from the dropdown list.

18. Click the **Next Step** button.
19. Select the **Display in Portal** checkbox on the **Portal Display** page.
20. Enter descriptive text about the application in the **Application Tooltip** field. The portal will display this text when a user passes the cursor over the application's icon.
21. Click the **Save and Finish** button.



22. Click the **Publish Changes** button in the top left corner of the page.

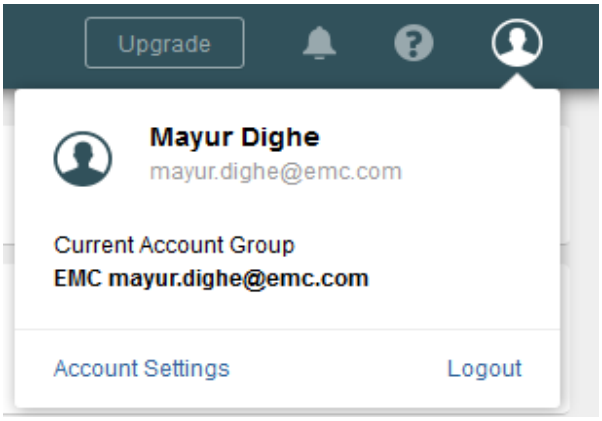


Configure ThousandEyes to Use RSA SecurID Access as an Identity Provider

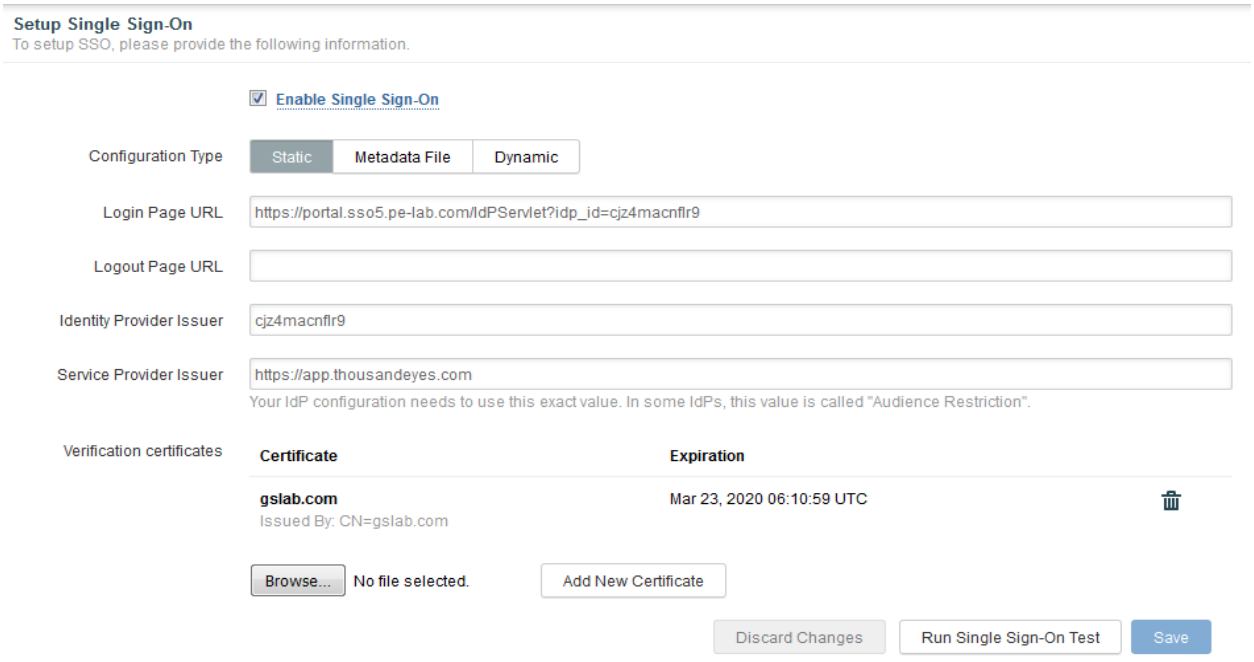
Follow below steps to configure ThousandEyes as service provider.

Create an Identity Provider

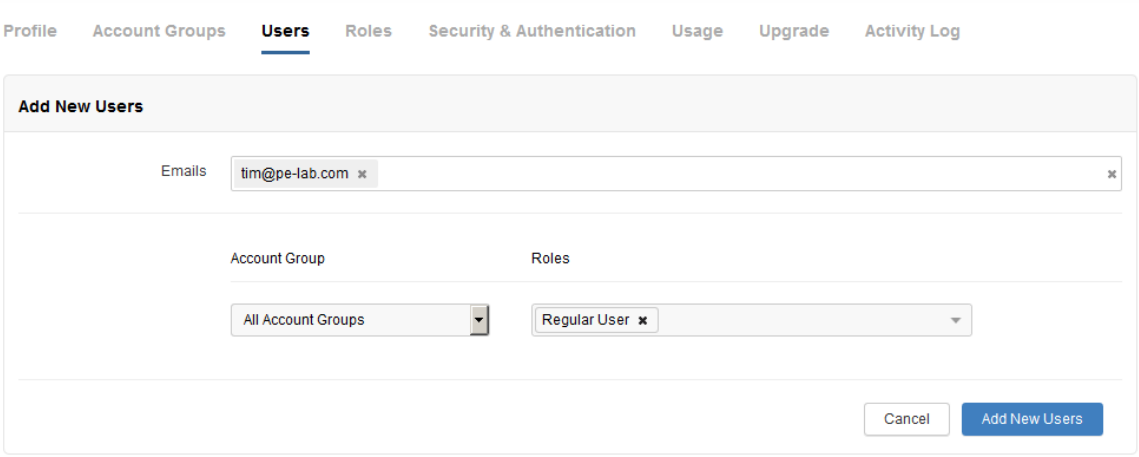
1. Log in to your ThousandEyes account and select **Account Settings** from the upper right corner of the page.



2. Click **Security & Authentication** option from tabs.
3. Check **Enable Single Sign-On**.
4. Then select **Configure Type** as **Static.**
5. Enter your RSA SecurID Access Identity Provider URL in the **Login Page URL** field.
6. (Optional) If you want ThousandEyes to redirect users to a custom URL after they log out, enter the URL in the **Logout Page URL** field.
7. Enter your ThousandEyes SP Issuer ID in the **Identity Provider Issuer** field.
8. Upload same public certificate which you imported while configuring RSA SecurID Access.
9. Click **Run Single Sign On Test** to check configurations.
10. Click **Save.**



11. Select the **Users** tab.
12. Select **Add New Users**.



13. The user will receive an email to complete registeration.

MD