RSA SecurID Access SAML Configuration for PagerDuty

Last Modified: September 16, 2015

PagerDuty provides alerting, on-call scheduling, escalation policies and incident tracking to increase uptime of your apps, servers, websites and databases.

Before You Begin

- Acquire PagerDuty account.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the SecurID Access manual.

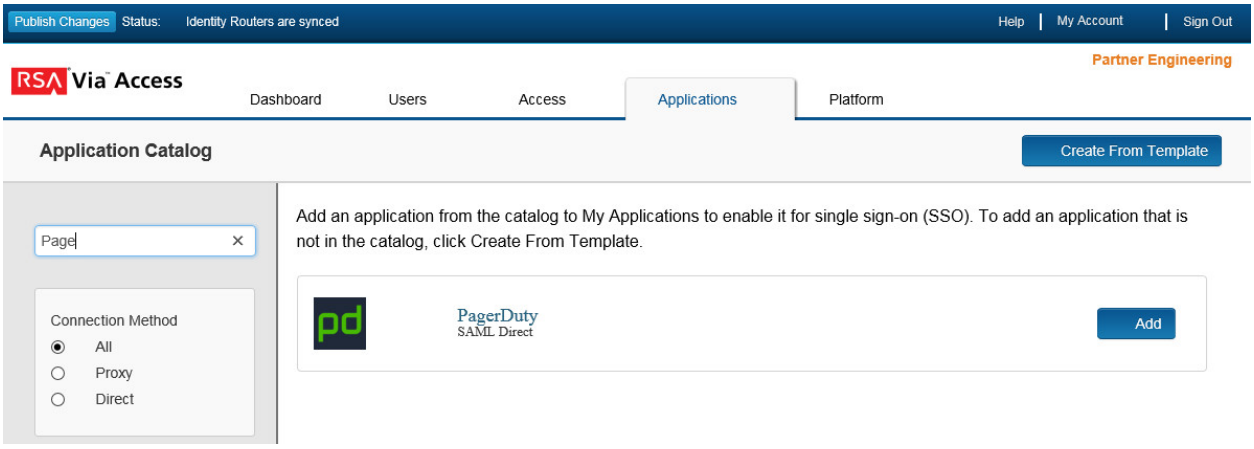
Procedure

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

Add the Application in RSA SecurID Access

Procedure

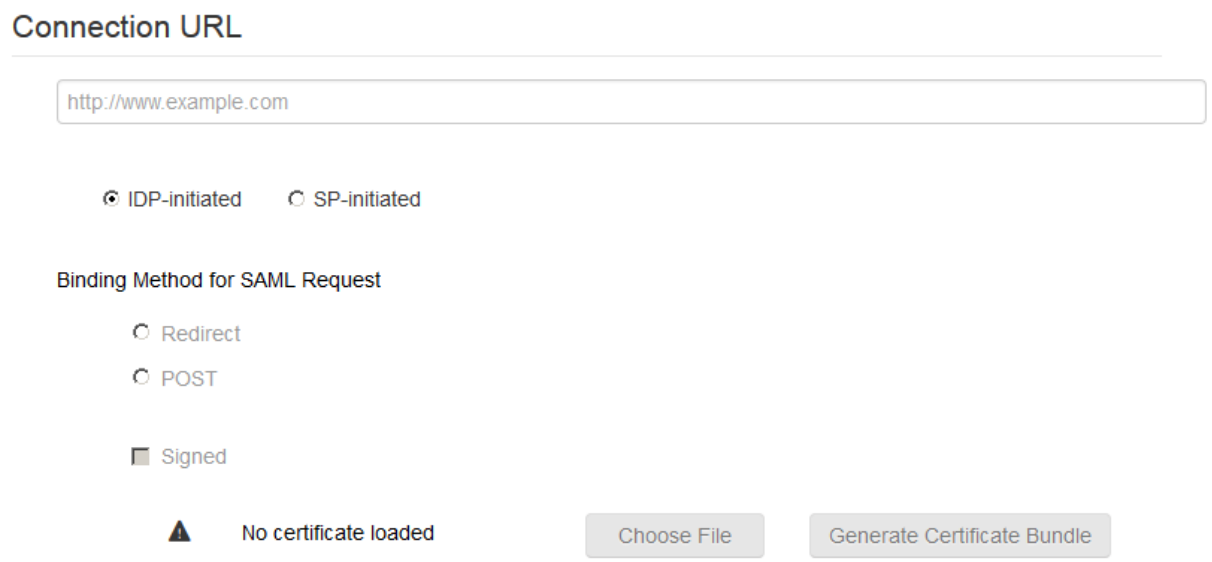
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the PagerDuty application.



3. On the Basic Information page, specify the application name and click **Next Step**.

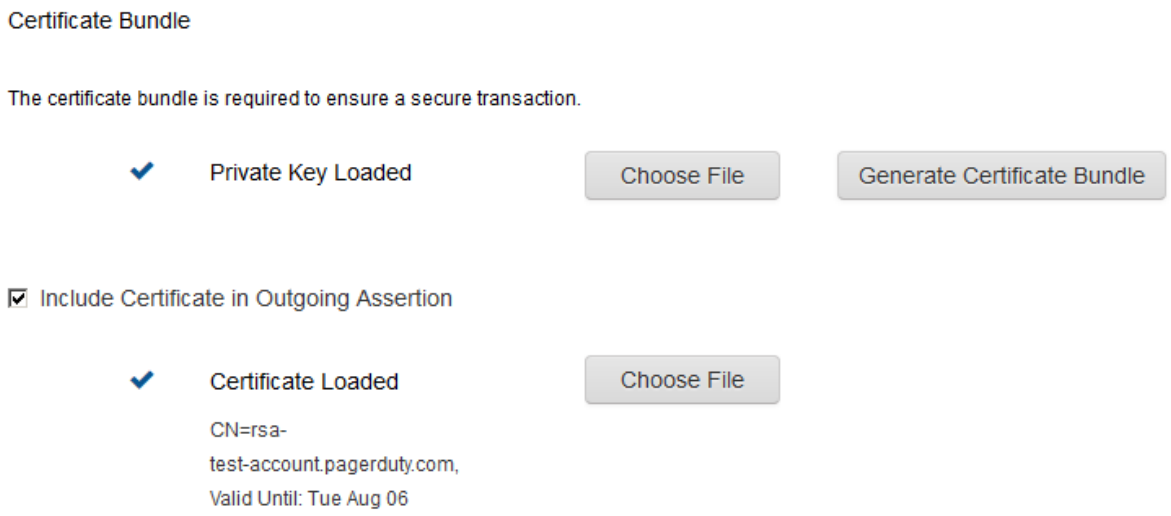
Note: The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.

4. On the Connection Profile page, choose **IDP-initiated** and leave the **Connection URL** blank.

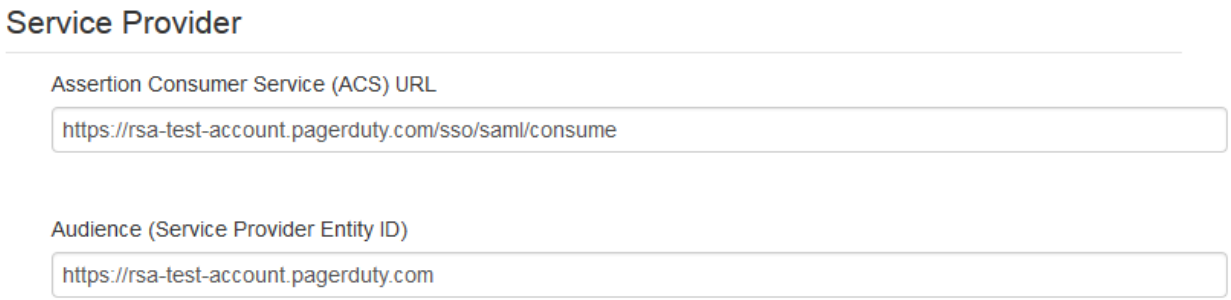


5. Scroll down to **SAML Identity Provider (Issuer)** section.
6. Take note of the Identity Provider URL it will be needed later to configure PagerDuty.

7. Click **Choose File** and upload the RSA SecurID Access private key.
8. Select the checkbox **Include Certificate in Outgoing Assertion**.
9. Click **Choose File** and upload the cert.pem public certificate.

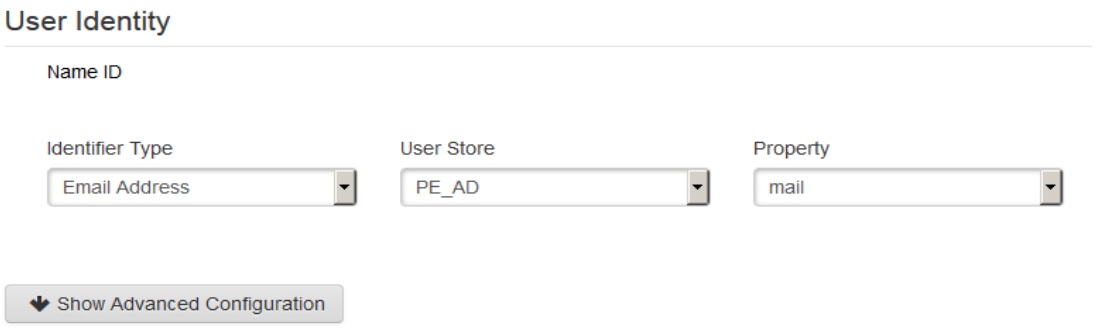


10. Scroll down to the **Service Provider** section.



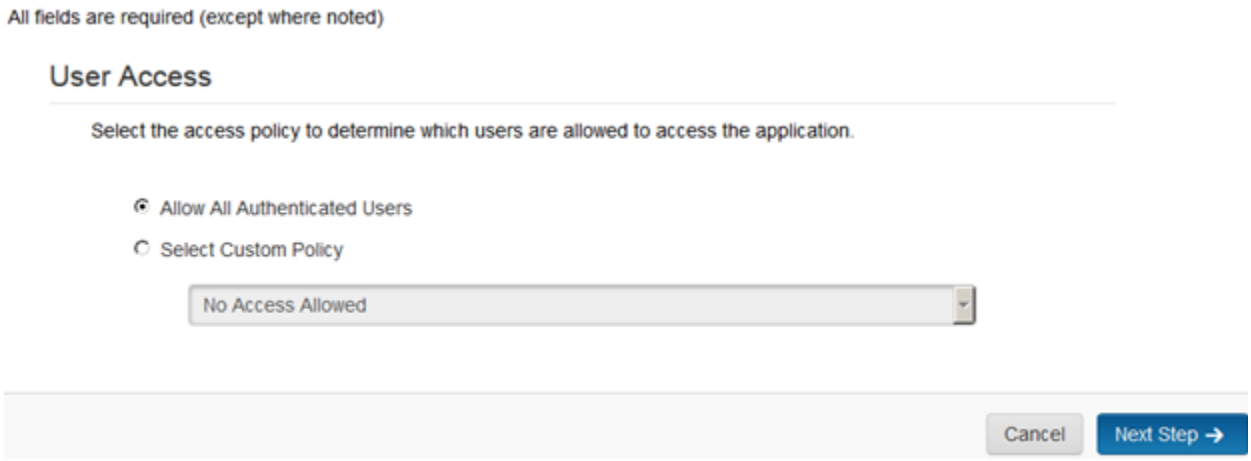
    a. In the **Assertion Consumer Service (ACS) URL** field, enter https://<your_instance>.pagerduty.com/sso/saml/consume
    b. In the **Audience (Service Provider Entity ID)** field, enter https://<your_instance>.pagerduty.com

11. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

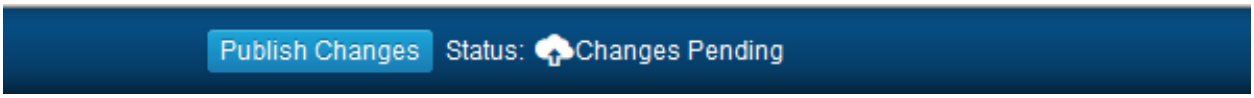


12. Click **Next Step**.

13. On the **User Access** page, select the desired user policy from the drop down list.



14. Click **Next Step**.
15. On the Portal Display page, select **Display in Portal**.
16. Click **Save and Finish**.
17. Click **Publish Changes**. Your application is now enabled for SSO.



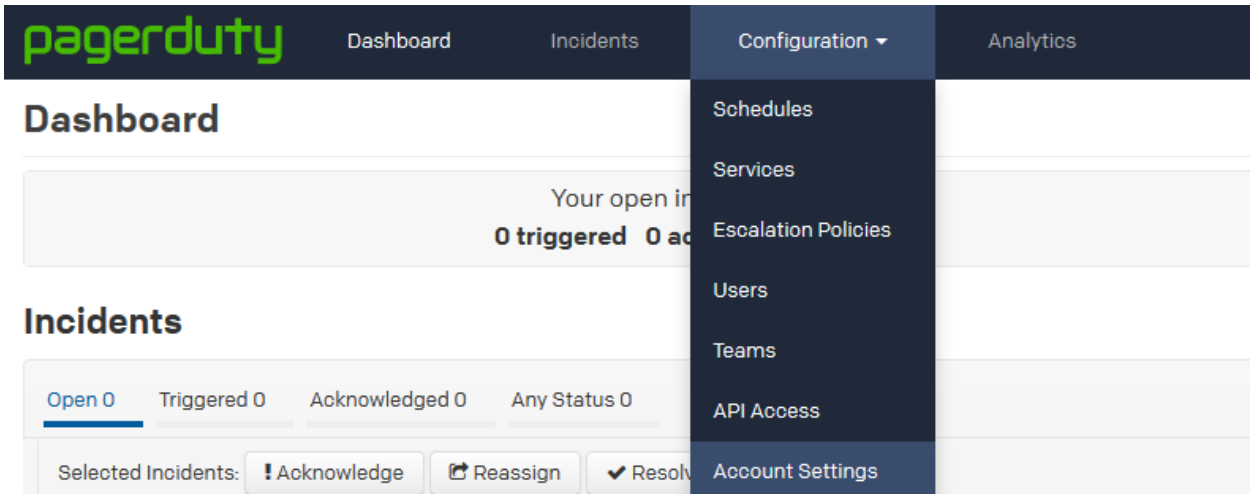
Next Steps

[Configure PagerDuty to Use RSA SecurID Access as an Identity Provider]

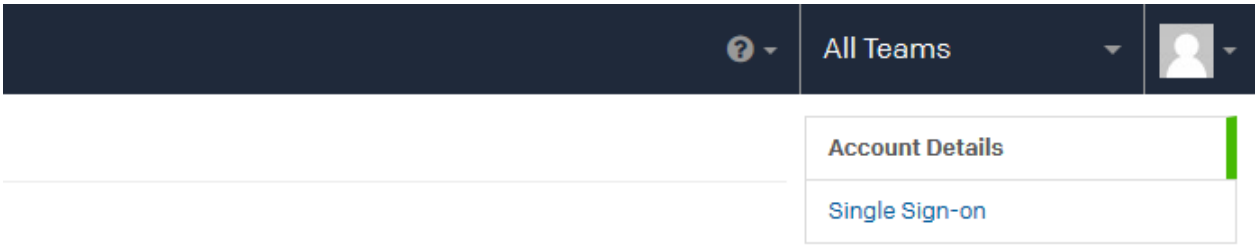
Configure PagerDuty to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to the PagerDuty Admin Console. https://<your_instance>.pagerduty.com/sign_in
2. Navigate to **Configuration > Account Settings**.

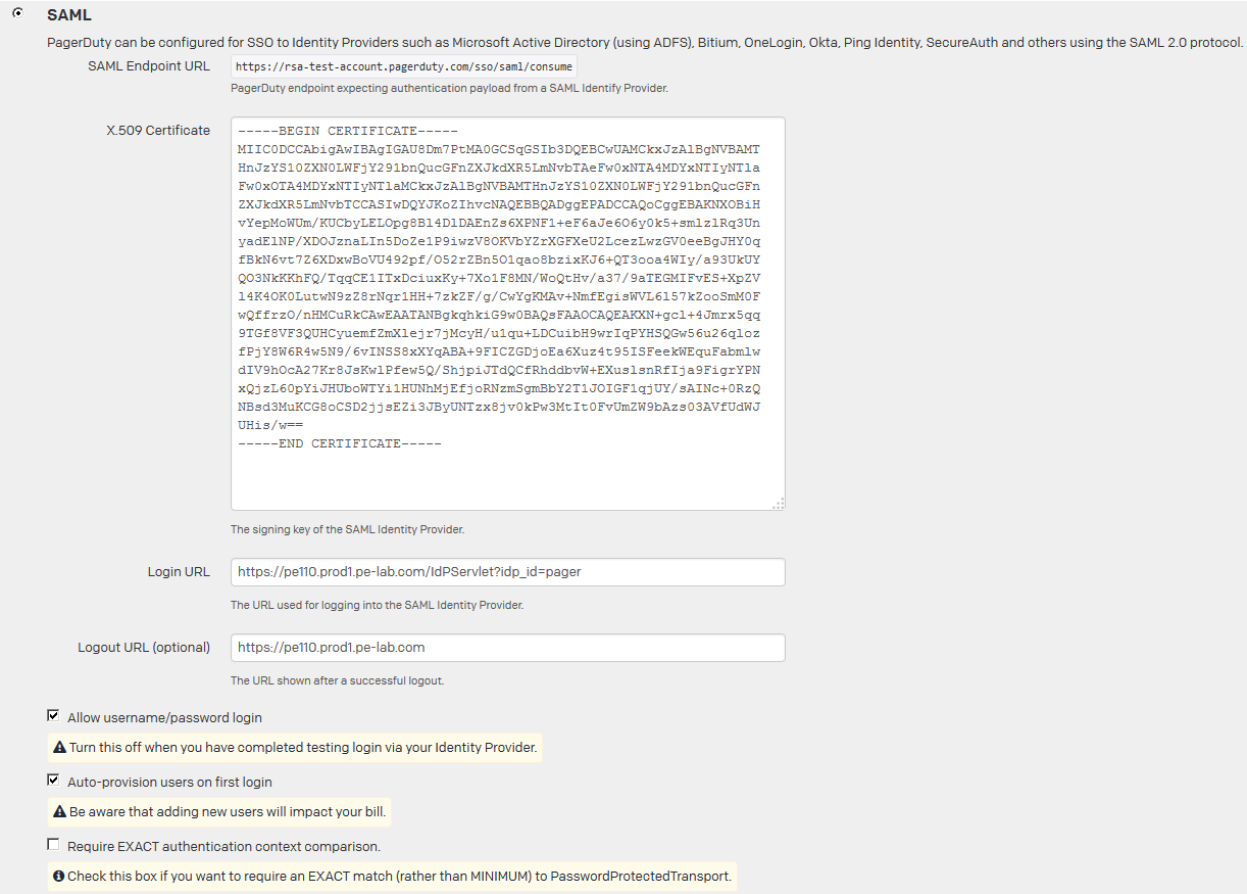


3. Click on **Single Sign-on.**



4. Select the **SAML** radio button.

5. Take not of the SAML Endpoint URL, this is the ACS URL on the RSA SecurID Access.



6. Paste the RSA SecurID Access **x.509 certificate** into the window including the ---Begin and End lines.
7. Enter the **Identity Provider URL** from step 6 into the Login URL field.
8. If you would like the users to still be able to login with their username and password that is not managed by RSA SecurID Access then check **Allow Username/password login**.
9. Manually configure a user or check the **Auto-provision users on first login**.
10. Click **Save Changes**.

GLS