

**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.

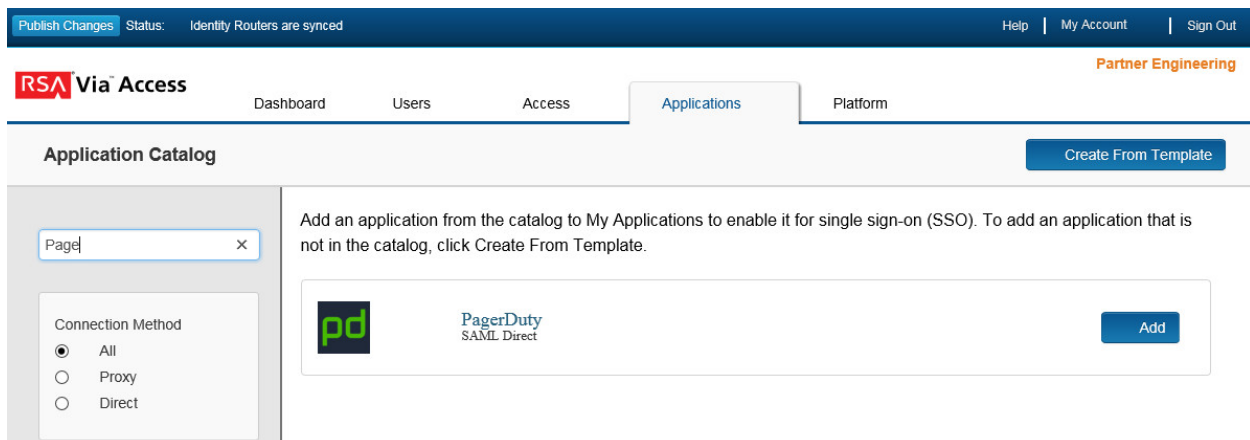
## Procedure

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.



The screenshot shows the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with "Publish Changes", "Status: Identity Routers are synced", "Help", "My Account", and "Sign Out". Below this is the "RSA Via Access" header with navigation tabs for "Dashboard", "Users", "Access", "Applications", and "Platform". The "Applications" tab is active. The main content area is titled "Application Catalog" and includes a "Create From Template" button. On the left, there is a search box containing "Page1" and a "Connection Method" section with radio buttons for "All" (selected), "Proxy", and "Direct". The main area displays a list of applications, with one application visible: "PagerDuty SAML Direct" with a logo and an "Add" button. A descriptive text above the list states: "Add an application from the catalog to My Applications to enable it for single sign-on (SSO). To add an application that is not in the catalog, click Create From Template."

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.

### Connection URL

---

IDP-initiated    SP-initiated

#### Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

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.

### SAML Identity Provider (Issuer)

---

Identity Provider URL

Issuer Entity ID

Default (idp\_id): pager

Override

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.

#### Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

✓ Private Key Loaded

Choose File

Generate Certificate Bundle

Include Certificate in Outgoing Assertion

✓ Certificate Loaded

Choose File

CN=rsa-  
test-account.pagerduty.com,  
Valid Until: Tue Aug 06

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

#### Service Provider

Assertion Consumer Service (ACS) URL

<https://rsa-test-account.pagerduty.com/sso/saml/consume>

Audience (Service Provider Entity ID)

<https://rsa-test-account.pagerduty.com>

- 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**.

#### User Identity

Name ID

Identifier Type

Email Address

User Store

PE\_AD

Property

mail

⌵ Show Advanced Configuration

12. Click **Next Step**.

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

All fields are required (except where noted)

### User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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.

Publish Changes

Status:  Changes Pending

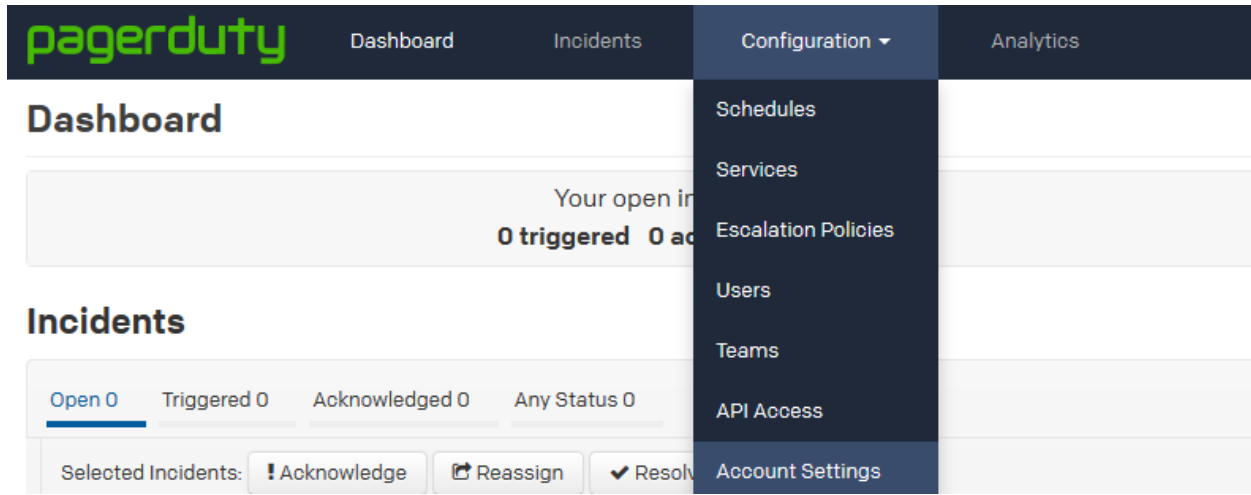
### Next Steps

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

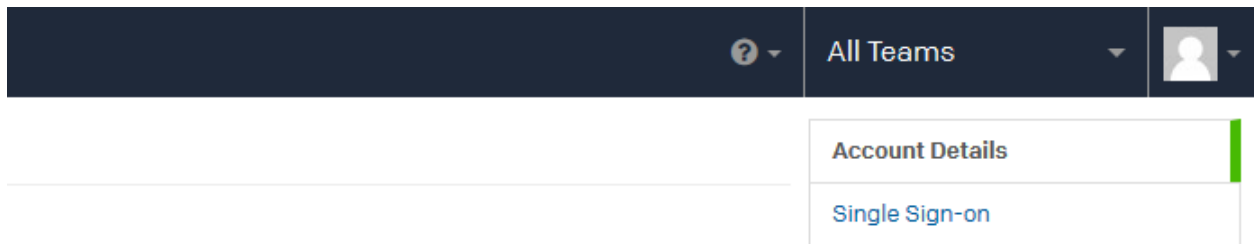
# Configure PagerDuty to Use RSA SecurID Access as an Identity Provider

## Procedure

1. Login to the PagerDuty Admin Console. [https://<your instance>.pagerduty.com/sign\\_in](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 note of the SAML Endpoint URL, this is the ACS URL on the RSA SecurID Access.

**SAML**

PagerDuty can be configured for SSO to Identity Providers such as Microsoft Active Directory (using ADFS), Bitium, OneLogin, Okta, Ping Identity, SecureAuth and others using the SAML 2.0 protocol.

SAML Endpoint URL   
PagerDuty endpoint expecting authentication payload from a SAML Identity Provider.

X.509 Certificate 

```
-----BEGIN CERTIFICATE-----
MIIC0DCCAbigAwIBAgI GAU8Dm7PtMA0GCSqGSIb3DQEBCwUAMCkxJzA1BgnVBAMT
HnJzYS10ZXN0LWFjY291bnQucGFuZG9kbWVudC50aW50eS01aW50eS01aW50eS01
Fw0xOTA4MDYxNTIyNTI1aMcKxJzA1BgnVBAMT HnJzYS10ZXN0LWFjY291bnQucGFu
ZXJkdXR5LmVudC50aW50eS01aW50eS01aW50eS01aW50eS01aW50eS01aW50eS01
vYepMoWUm/KUCbyLELOpg8B14D1DAEnZs6XPNF1+eF6aJe606y0k5+sm1z1Rq3Un
yadE1NF/XDOJznaLin5Do2e1P9iWzV8OKVbYZrXGFxeU2LcezLwzGV0eeBgJHY0q
fBkN6vt7Z6XDxwBoVU492pf/052z2Bn501qao8bzixKJ6+QT30oa4WIy/a93UkUY
QO3nkKKhFQ/TqqCE1ITxDoc1uxKy+7Xo1F8MN/WoQcHv/a37/9aTEGMIFvES+XpZV
14K4OK0LutwN9zZ8rNqr1HH+7zk2F/g/CwYgKMAV+NmfEg1sWVL6157kZooSmM0F
wQffrzO/nHMCuRkCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAkXN+gc1+4Jmrx5gq
9TGf8VF3QUHCyuemfZmX1ejr7jMcyH/u1qu+LDCuibH9wrIqPYH5Q9w56u26qloz
fPjY8W6R4w5N9/6vINSS8xYqABA+9FICZGDjoeEa6Xuz4t95ISFeeKWEquFabmlw
dIV9hOoA27Rr8Jskw1Pfew9Q/ShjpiJtdQCfRhddebvW+EXus1enRfIja9FigrYFN
xQJzL60pYiJHUb0WTYi1HUNhMjE.Fj0RNzmSgmBbY2T1JOIGF1qjUY/sAInC+0RzQ
NBsd3MuKCG8oCSD2jjseEz13JByUNTzx8jv0kPw3MctIt0FvUmZW9bAzs03AVFUDWJ
UH1s/w==
-----END CERTIFICATE-----
```

The signing key of the SAML Identity Provider.

Login URL   
The URL used for logging into the SAML Identity Provider.

Logout URL (optional)   
The URL shown after a successful logout.

Allow username/password login  
▲ Turn this off when you have completed testing login via your Identity Provider.

Auto-provision users on first login  
▲ Be aware that adding new users will impact your bill.

Require EXACT authentication context comparison.

Check this box if you want to require an EXACT match (rather than MINIMUM) to PasswordProtectedTransport.

- Paste the RSA SecurID Access **x.509 certificate** into the window including the ---Begin and End lines.
- Enter the **Identity Provider URL** from step 6 into the Login URL field.
- 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**.
- Manually configure a user or check the **Auto-provision users on first login**.
- Click **Save Changes**.