# Privileged Account Management (PAM)

## Virtual Desktop Service

Toby vanRoojen
November 20, 2020

# Table of Contents

# Privileged Account Management (PAM)

## Privileged Account Management (PAM)

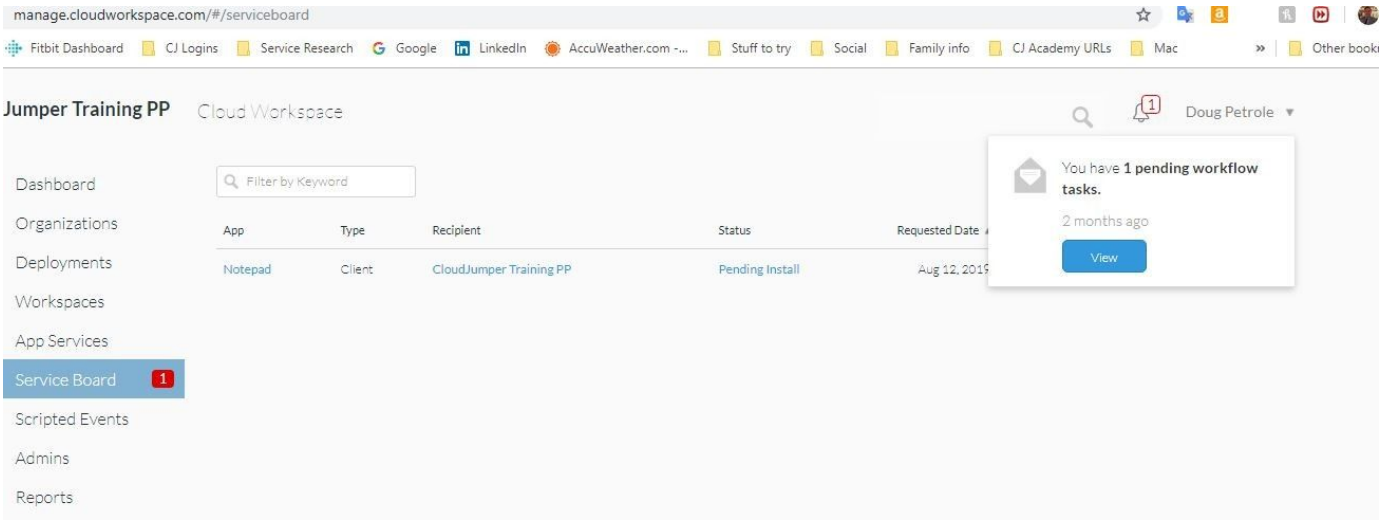
This feature provides a specific, audit-able record of granular administrative permission sets granted to VDS and/or Active Directory privileged accounts. External access automatically expires by default.

PAM provides a mechanism to allow Customers to grant the VDS administrator and/or NetApp VDS Support access and a method for Customers to grant Partners access in an auditable, trackable, reportable format for compliance purposes.

In the modern security context, every privileged account must have a purpose (and as specific a purpose as possible) and should only remain active when needed to reduce attack surface.

## Approving and Rejecting PAM Requests in VDS

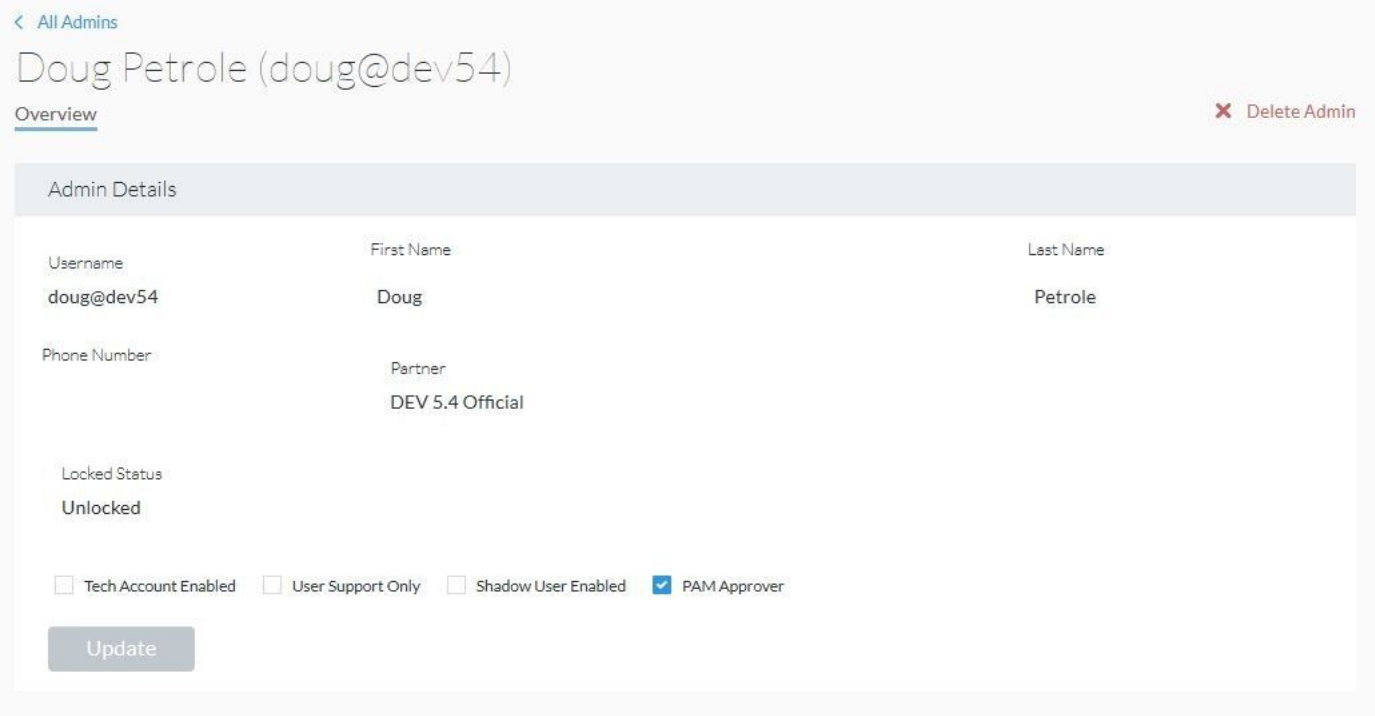
Once a PAM request is made all VDS admins will be able to see an alert under the bell.




all VDS admins can view PAM requests, but only admins with the PAM approver role will be able to approve or reject requests.

Applying the PAM Approver Role

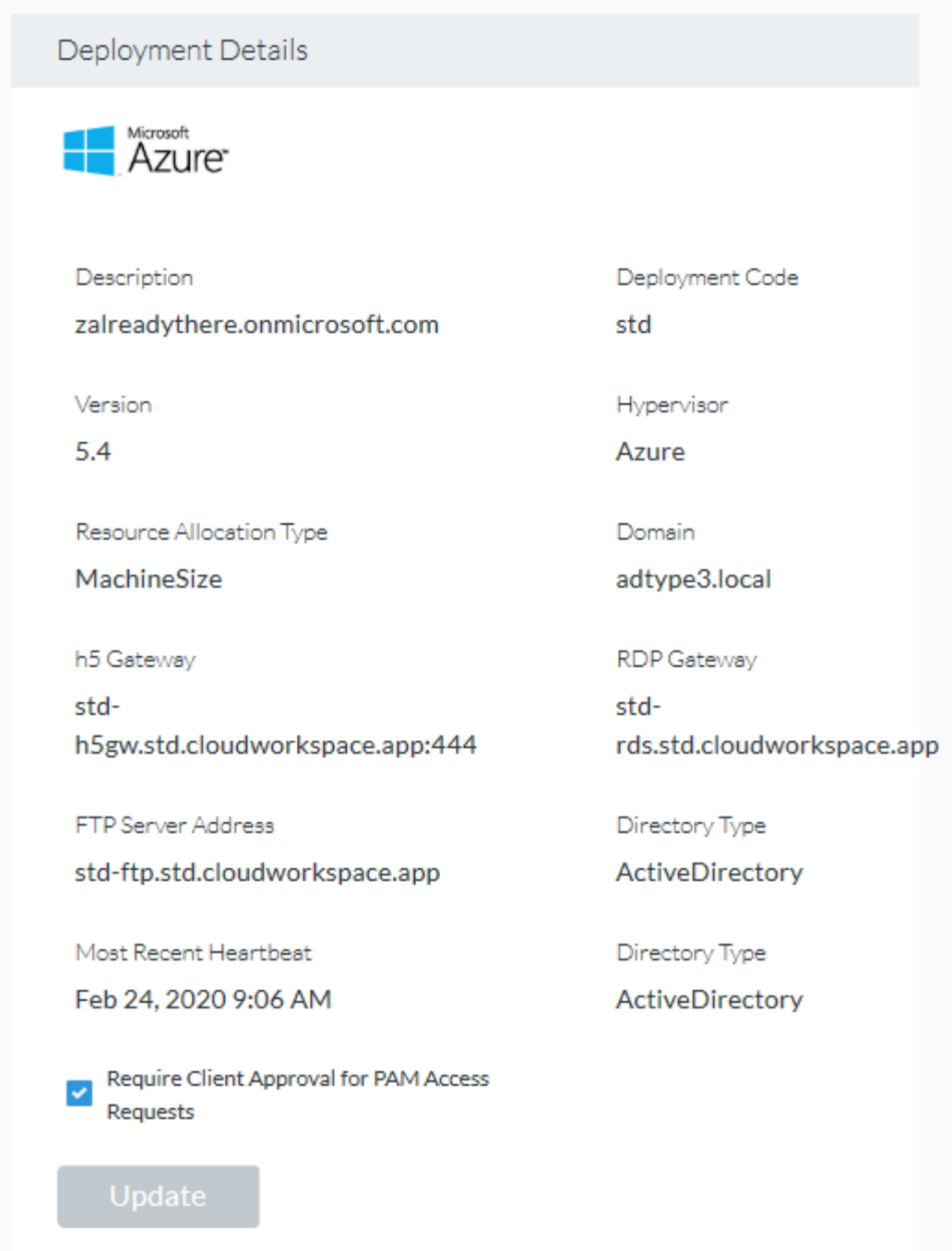
All Primary Admins will inherit the PAM Approver role, but this role can be assigned to any other VDS admin as long as the VDS user has Admin - Edit permissions. Navigate to the Admins module, select an admin and check the box for PAM Approver.




Turning on Client-Level Approvals

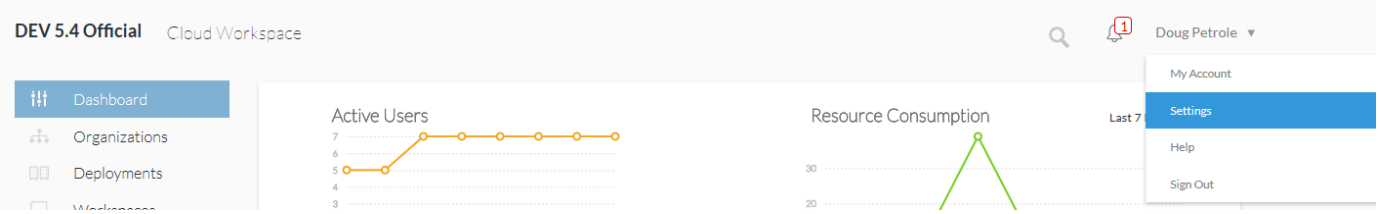
In the event that an organization's deployment requires the ability to approve access as well, Software Master Partners can turn on Client-level approvals by navigating to the Deployments module and scrolling down to the Deployment Details section.

Next, check the box that reads Require Client Approval for PAM Access Requests and click Update. This will send requests that the Software Master Partner requests through to the VDS admins for the deployment. Note: this requires that users are set up as VDS admins as well via these steps. <[Link to Admin Access for Users]




Approving/Rejecting PAM Requests

All admins can view requests by clicking the drop-down arrow next to their name, then Settings, then the PAM Requests tab. Note: Client level approvals see the same information and follow the same process defined below.




Admins can review the following details of each request prior to clicking the settings wheel for each request

and approving or rejecting it:

Request ID: useful to know when communicating/tracking requests, or for reference when auditing access to your environment

Access Level:

VDS: grants full permissions as a VDS admin

Deployment: grants Domain Admin level access to the Active Directory structure for troubleshooting purposes

Requester: the email address of the person requesting access

Deployment: the deployment identifier the requester has asked for privileged access to

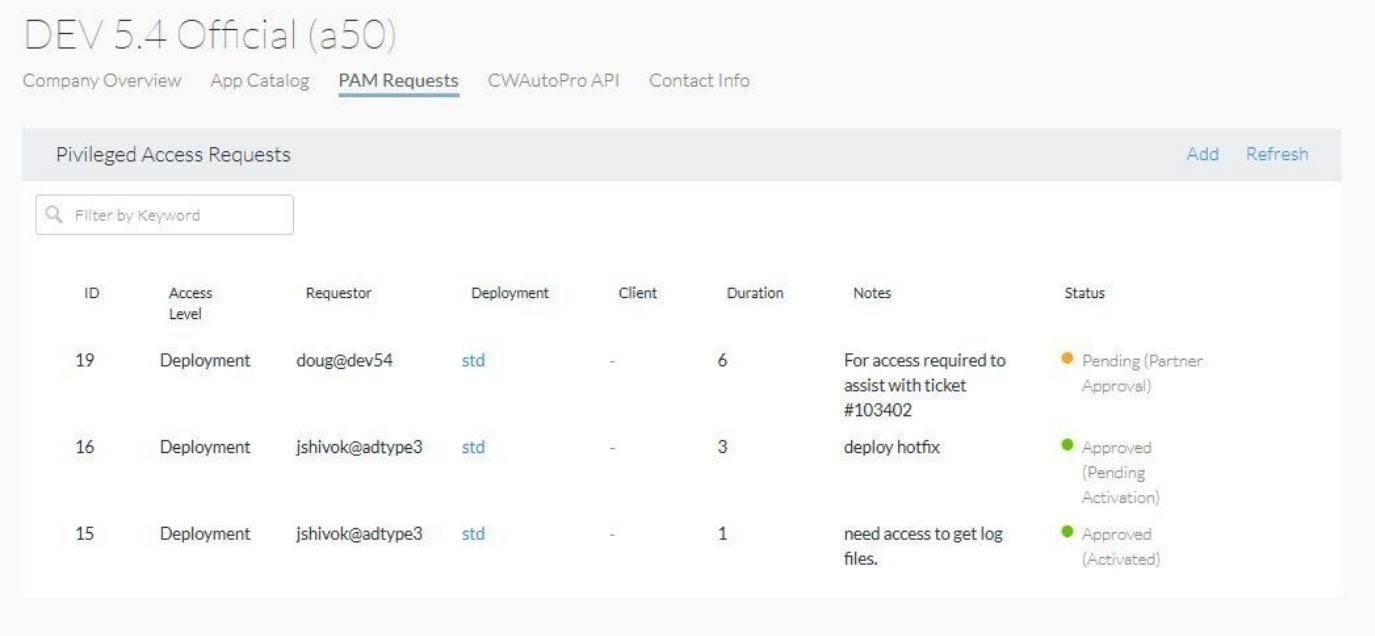
Duration: the number of days this access will be active prior to automatically expiring (defaults to 3)

Notes: displays all notes that were entered by the requester

Status:

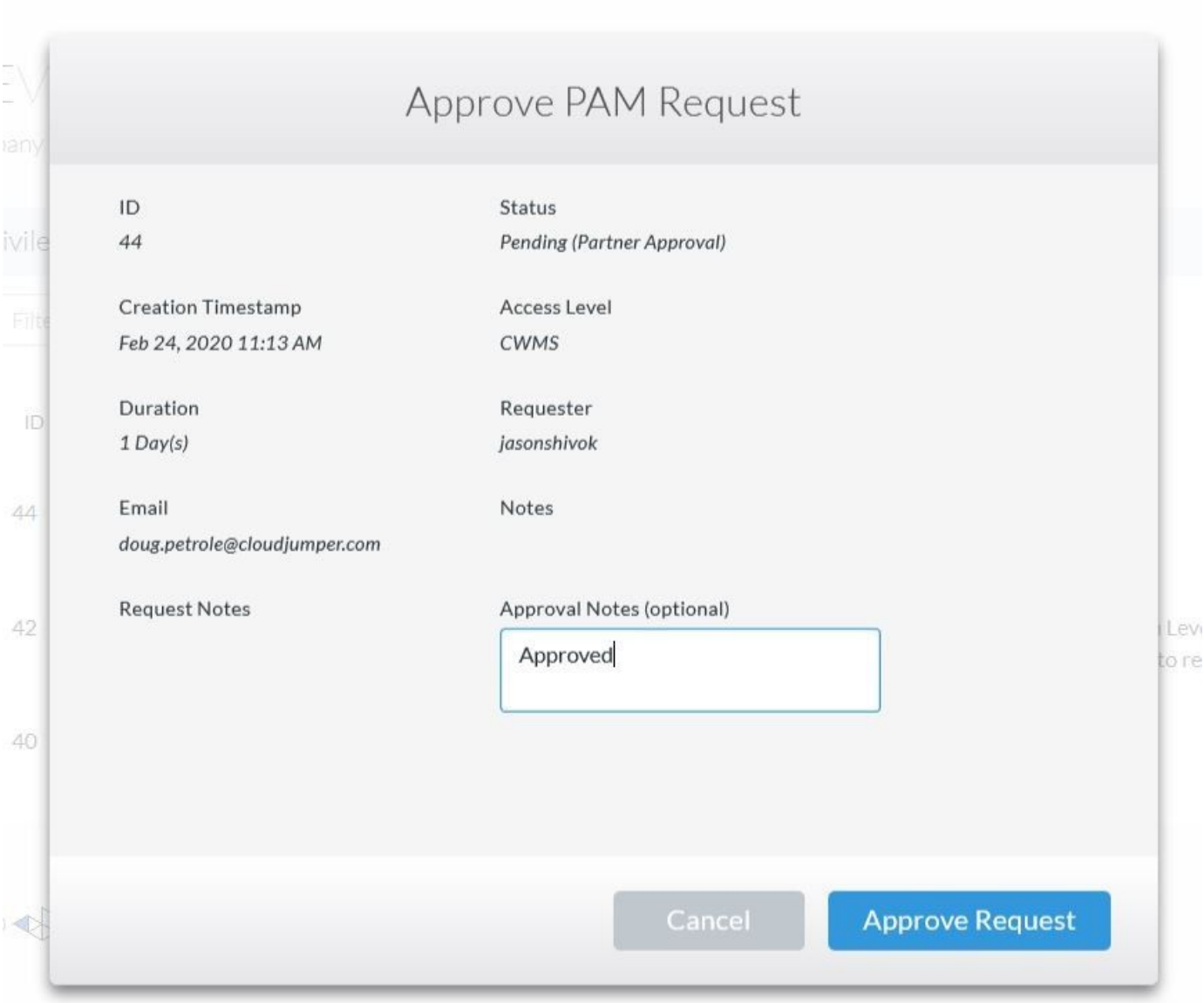
Pending Approval: displays requests that have yet to be approved or rejected by a PAM approver

Approved: displays existing, approved requests




Approving

After clicking the settings wheel PAM approvers will see the request details again. The PAM approver can then enter any notes required for the recipient and click Approve to grant temporary, audited access.

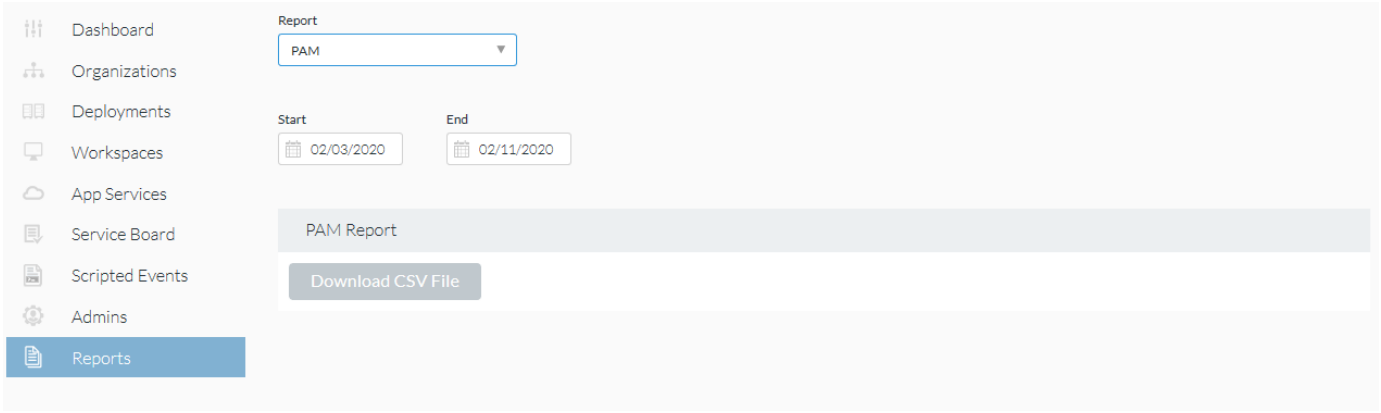



Rejecting

VDS Admins can enter notes when rejecting PAM requests. An example of this would be asking that the requester ask for the same permissions, but for a shorter duration.


Reporting on PAM Requests

VDS Admins with Reporting rights can navigate to the Reports module and export a csv file displaying all of the details surrounding every PAM request.




Activating PAM Accounts

The email account entered when creating the PAM request will receive the following message. Click Activate Request to gain the administrative access (Active Directory for the Deployment) requested.

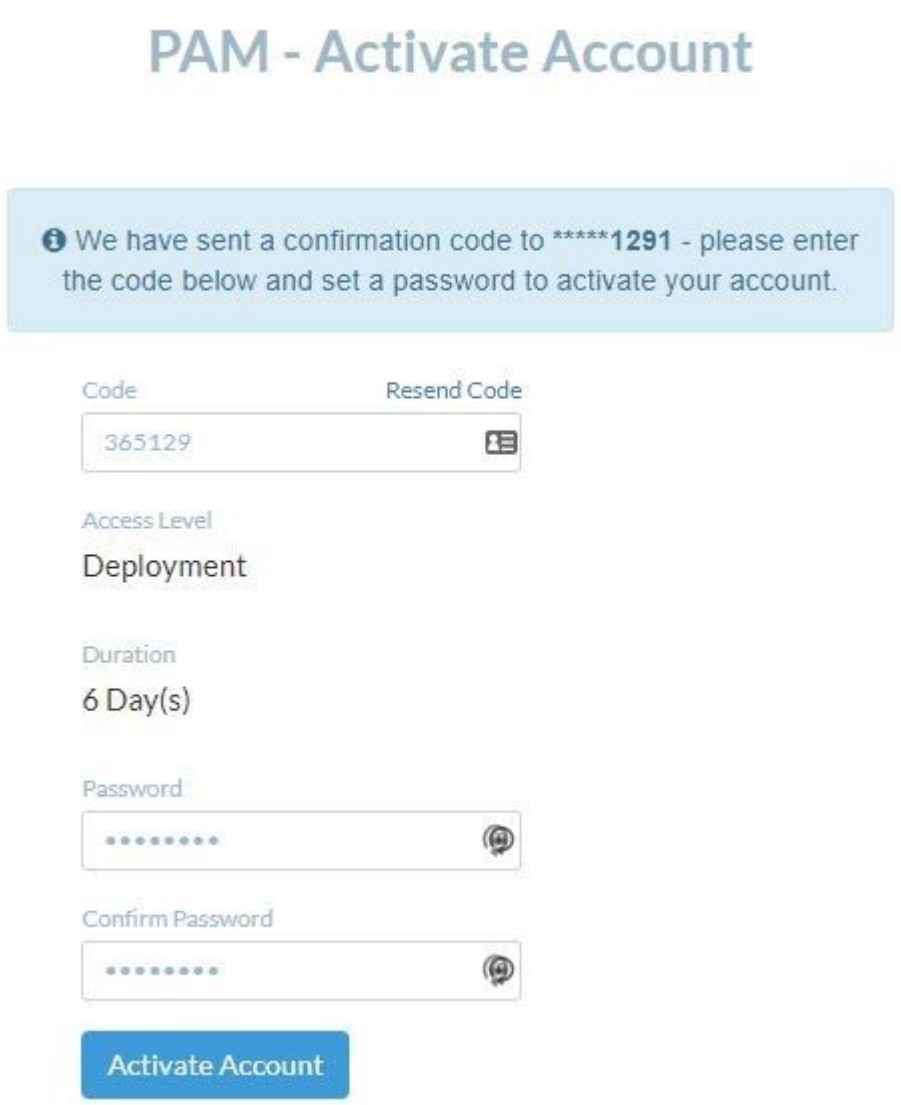
Dear doug.petrole@cloudjumper.com
Your request for Deployment(std) access has been approved by doug@dev54.
Please use the link below to activate your temporary account.

Activate Request

Notes from the approver:
no notes provided

Clicking Activate Request will send an SMS message to the number entered when creating the PAM request.

Enter the code that you receive on your mobile device, then set the password for your Active Directory account for the deployment.




You will then see that the Active Directory admin account for this deployment has been successfully created.


Expired Accounts

Accounts that expire will receive a message similar to the following, at which point the privileged access associated with this email address will no longer be in effect.

Dear doug.petrole@cloudjumper.com
Your access to Deployment() has expired after 6 days.
Please submit another request for access if this is still required.