



Privileged Account Management (PAM)

Virtual Desktop Service

Toby vanRoojen
November 20, 2020

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Management.System_Administration.privileged.account.management.html on December 10, 2020. Always check docs.netapp.com for the latest.



Table of Contents

- Privileged Account Management (PAM) 1
 - Privileged Account Management (PAM) 1
 - Approving and Rejecting PAM Requests in VDS 1

Privileged Account Management (PAM)

Privileged Account Management (PAM)

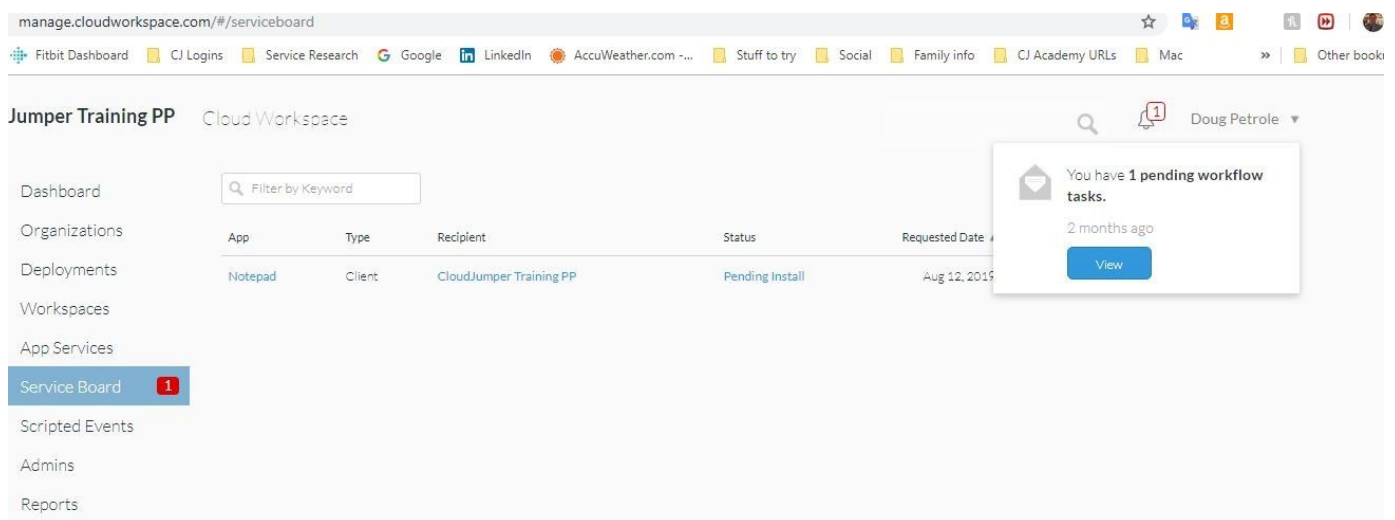
This feature provides a specific, audit-able record of granular administrative permission sets granted to VDS and/or Active Directory privileged accounts. External access automatically expires by default.

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.



The screenshot shows the 'manage.cloudworkspace.com/#/serviceboard' interface. On the left is a sidebar with navigation links: Dashboard, Organizations, Deployments, Workspaces, App Services, Service Board (highlighted with a red badge '1'), Scripted Events, Admins, and Reports. The main area displays a table of requests with columns: App, Type, Recipient, Status, and Requested Date. A single request is visible: App 'Notepad', Type 'Client', Recipient 'CloudJumper Training PP', Status 'Pending Install', and Requested Date 'Aug 12, 2019'. A notification bubble in the top right corner states 'You have 1 pending workflow tasks. 2 months ago' with a 'View' button. The top right of the interface shows a search icon, a bell icon with a red badge '1', and the user name 'Doug Petrole'.

App	Type	Recipient	Status	Requested Date
Notepad	Client	CloudJumper Training PP	Pending Install	Aug 12, 2019



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.

< All Admins

Doug Petrole (doug@dev54)

Overview

✖ Delete Admin

Admin Details

Username	First Name	Last Name
doug@dev54	Doug	Petrole

Phone Number	Partner
	DEV 5.4 Official

Locked Status

Unlocked

☐ Tech Account Enabled ☐ User Support Only ☐ Shadow User Enabled ☒ PAM Approver

Update

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](#)>

Deployment Details

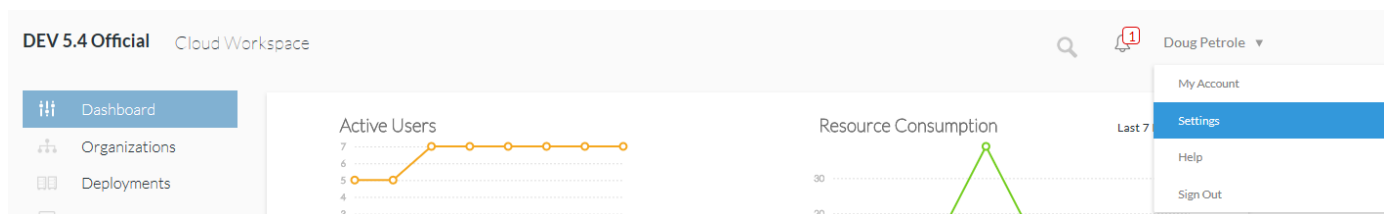


Description	Deployment Code
zalreadythere.onmicrosoft.com	std
Version	Hypervisor
5.4	Azure
Resource Allocation Type	Domain
MachineSize	adtype3.local
h5 Gateway	RDP Gateway
std- h5gw.std.cloudworkspace.app:444	std- rds.std.cloudworkspace.app
FTP Server Address	Directory Type
std-ftp.std.cloudworkspace.app	ActiveDirectory
Most Recent Heartbeat	Directory Type
Feb 24, 2020 9:06 AM	ActiveDirectory
<input checked="" type="checkbox"/> Require Client Approval for PAM Access Requests	

Update

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

DEV 5.4 Official (a50)

Company Overview

App Catalog

PAM Requests

CWAutoPro API

Contact Info

Privileged Access Requests

Add

Refresh

Filter by Keyword

ID	Access Level	Requestor	Deployment	Client	Duration	Notes	Status
19	Deployment	doug@dev54	std	-	6	For access required to assist with ticket #103402	<div>Pending (Partner Approval)</div>
16	Deployment	jshivok@adtype3	std	-	3	deploy hotfix	<div>Approved (Pending Activation)</div>
15	Deployment	jshivok@adtype3	std	-	1	need access to get log files.	<div>Approved (Activated)</div>

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.

Approve PAM Request

ID	Status
44	Pending (Partner Approval)

Creation Timestamp	Access Level
Feb 24, 2020 11:13 AM	CWMS

Duration	Requester
1 Day(s)	jasonshivok

Email	Notes
doug.petrole@cloudjumper.com	

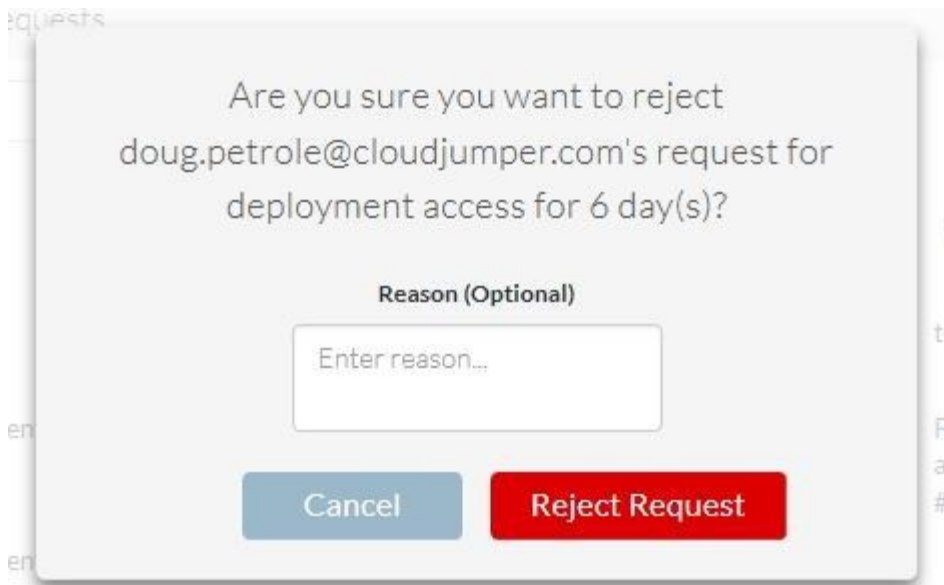
Request Notes	Approval Notes (optional)
	<input type="text" value="Approved"/>

Cancel

Approve Request

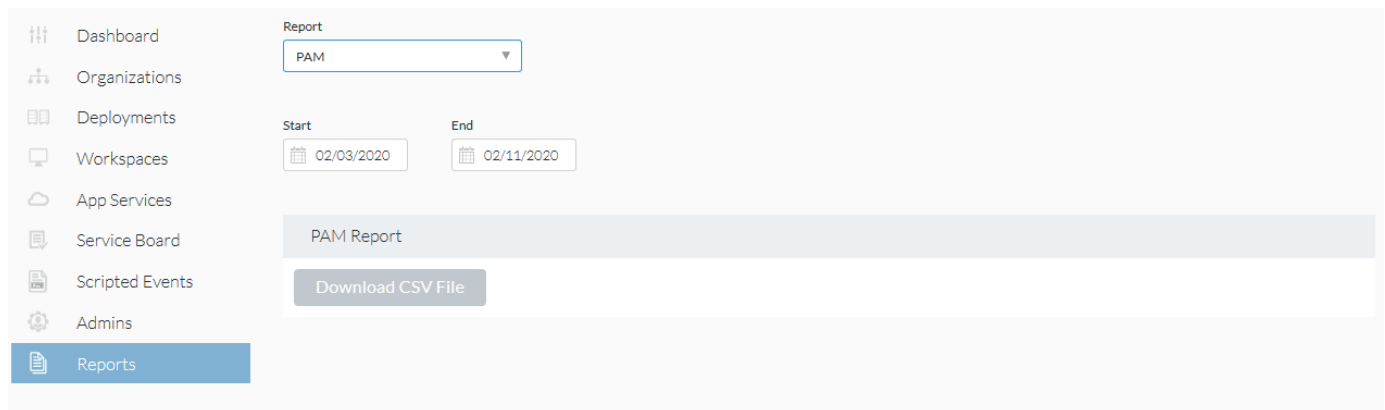
Rejecting

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.

PAM - Activate Account

 We have sent a confirmation code to *****1291 - please enter the code below and set a password to activate your account.

Code Resend Code
 

Access Level
Deployment

Duration
6 Day(s)

Password
 

Confirm Password
 

Activate Account

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

PAM - Activate Account

 Successfully activated account. Your account's username is **doug.petrole@adtype3.local**.

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.

Copyright Information

Copyright © 2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.