# Virtual Desktop Managed Service Documentation

## Virtual Desktop Managed Service

NetApp
July 30, 2021

# Table of Contents

# Virtual Desktop Managed Service Documentation

## Overview

NetApp's Virtual Desktop Managed Service (VDMS) solves the complexity of deploying and managing virtual desktops in the public cloud, delivered as a managed VDI as a Service platform.

## Getting support

Email support: VDSsupport@netapp.com

Phone Support: 844.645.6789

VDMS Support Portal

Normal support business hours: Monday-Friday, 7:00am-7:00pm Central Time.

- After hours (on-call) support available via phone only.

## Windows Virtual Desktop (WVD) clients

- Microsoft WVD for Windows client
- Microsoft WVD web client
- Microsoft WVD for Android client
- Microsoft WVD for macOS client
- Microsoft WVD for iOS client

## Service Components

VDMS is a co-managed service offering that brings together multiple technologies from NetApp and Microsoft and applies best-practices learned over 20+ year in the EUC market. Below a selected list of components are listed. Not all components are used in all deployments due to varying customer requirements.

### NetApp

- NetApp SaaS Backup
  - Licensing for NetApp's SaaS backup service is included in VDMS.
- Azure NetApp Files (ANF)
  - The data storage layer for deployments with more than 49 users is based on ANF.
  - For deployments with <250 users the standard performance tier is used.
  - For deployments with >249 users the premium performance tier is used.
- NetApp Cloud Backup
  - NetApp Cloud Backup is used to backup ANF storage volumes.
- NetApp Cloud Sync
  - NetApp Cloud Sync can be used to migrate data into VDMS when ANF is the data storage layer

technology.

- NetApp Cloud Insights
  - NetApp Cloud Insights is used by our support and services team for performance monitoring.
- NetApp VDMS Support
  - VDMS includes 24/7 incident support and in-boarding services provided by a specialized NetApp support team

## Microsoft

- Azure Files (AF)
  - The data storage layer for deployments with fewer than 50 users is based on AF technology. We configure the "transaction-optimized" tier in a GPv2 storage account.
  - For deployments with >49 users ANF is used.
- Azure Cloud Backup
  - Azure Cloud Backup is used to backup AF storage volumes and virtual machines.
- Azure File Sync
  - Azure File Sync can be used to migrate data into VDMS when AF is the data storage layer technology.
- Azure Defender
  - VDMS activates (and includes licensing for) Azure Defender, an advance security service on all virtual machines in the environment. Management and administration is performed via the Azure Security Center by the customer and/or their IT service provider. Managing Azure Security Center is not a service included in VDMS.
- Azure Virtual Machines
  - VDMS relies heavily on Windows-based Azure virtual machines for hosting user sessions and customer applications.
- Azure Virtual Network Peering
  - VDMS may leverage Azure virtual network peering to integrate with the customer's existing Active Directory Domain Controller (AD DC).
- Azure VPN
  - VDMS may leverage Azure site-to-site VPN to integrate with the customer's existing Active Directory Domain Controller (AD DC).
- Windows Virtual Desktop (WVD)
  - VDMS leverages native WVD functionality to support user session brokering, authentication, Windows licensing and more.
- Azure AD Connect
  - WVD requires that the local domain (AD DC) and Azure AD be in sync via the Azure AD Connect application.
- Microsoft 365 (M365)
  - WVD user sessions and Windows 10 Enterprise for the session hosts are licensed to the user via specific M365 license types. Assigning the appropriate M365 licensing to all VDMS users is a WVD and VDMS requirement. This licensing is not included in VDMS. It is the responsibility of the customer and/or their IT service provider to manage M365 licensing.

# Getting Started

## Virtual Desktop Managed Service (VDMS) prerequisites

### M365 Licensing

VDMS is built with Microsoft Windows Virtual Desktop (WVD) technology. WVD prerequisites require that the end users be assigned specific Microsoft 365 (M365) licensing. This licensing is not included in the VDMS subscription and NetApp does not sell or otherwise offer this license.

Responsibility for M365/WVD licensing compliance stays with the customer company, partner company and/or their M365 vendor.

There are a variety of M365 plans that support the WVD licensing for VDMS, details can be found here.

### M365/Azure AD Tenant

The customer must have an existing Azure AD tenant. Microsoft 365 is based on the same Azure AD tenant structure, therefore meeting the M365 Licensing requirement (above) will also satisfy this requirement.

### CSP Reseller Relationship

NetApp deploys VDMS into a dedicated Azure subscription using our CSP relationship with Microsoft. To deploy this subscription, NetApp needs to establish a reseller relationship with the customer's Azure AD tenant. A Global Admin for the customer's Azure AD tenant can accept this relationship here:

https://admin.microsoft.com/Adminportal/Home?invType=ResellerRelationship&partnerId=47c1f6d2-b112-48e0-915f-4304efffb3e8&msppId=0&DAP=true#/BillingAccounts/partner-invitation

Multi-partner functionality does not:

- Change any of the customer's existing subscriptions
- Transition the customer's existing subscriptions or account ownership
- Change the terms or customer's obligations for any of their existing subscriptions
- Change the partner of record for a subscription
- More details on this: https://docs.microsoft.com/en-us/partner-center/multipartner

#### Delegated Admin Rights

The invitation link (above) includes a request for delegated admin permissions. Acceptance will grant NetApp Global Admin and Helpdesk Admin roles in the customer's Azure AD tenant.

### Virtual Network Scope

VDMS will be deployed on a virtual network in Azure. The /20 IP range used for this network can not overlap with other networks in their environment.

In any scenario that adds network connectivity between the VDMS virtual network and any other customer network(s), overlap with another network IP range will break VDMS. Therefore it is vital that a completely unused /20 range be dedicated to VDMS.

The /20 network scope needs to land within one of these IP ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

## Deploy VDMS Worksheet

The customer/partner needs to complete the Deploy VDMS worksheet at:
https://www.deployvdms.com/

## Existing AD Integration

Integrating VDMS with an existing Active Directory domain controller (AD DC) requires several additional prerequisites:

#### Local Domain Admin Credentials

A local domain admin account with domainjoin rights, on the existing domain is required to establish the integration.

#### Azure AD Connect

WVD requires that Azure AD be synced with the AD DC using AD Connect. If this is not already setup, this utility will need to be installed and configured on your AD DC.

/=== Network Contributor Role for vNet Peering
/=== Local Gateway Device Admin Rights to setup VPN
/=== DNS Zones (need more tech info)
/=== no multi-domain forrest, Users must be in the domain we are deploying to

# Virtual Desktop Managed Service (VDMS) Service Summary

## User Resource Allocation

This article seeks to accurately describe the technical details of the VDMS service. Service details are subject to change and this article does not represent an amendment or alteration to any existing agreements, contracts or other arrangements between NetApp and any customers or partners.

#### Shared Users (SKU: VDMS-SUBS-SHARED-USER)

Shared user sessions run on a Session Host Virtual Machine (SHVM) with up to 10 user sessions. The total number of shared SHVMs allocated will ensure at least one shared SHVM for every 10 shared users in the environment.

**Resources allocated per shared user:**

- 8/10ths of a vCPU core
- 6.4 GiB RAM

- 25 GiB Storage

**Shared SHVM technical details:**

- Typically from the Esv3, Eav4 and Easv4 families of Azure virtual machines.
- 128 GiB Standard SSD OS disk
- Windows 10 Enterprise for Virtual Desktop
- FSLogix attached containers user profile
- Attached storage for company share

**VDI Users (SKU: VDMS-SUBS-VDI-USER)**

A VDI user's session runs on a dedicated Session Host Virtual Machine (SHVM) that does not concurrently host any other user sessions. The total number of VDI SHVMs is equal to the total number of VDI users in the environment.

**Resources allocated per VDI user:**

- 2 vCPU cores
- 8 GiB RAM
- 25 GiB Storage

**VDI SHVM technical details:**

- Typically from the Dsv3, Dav4 and Dasv4 families of Azure virtual machines.
- 128 GiB Standard HDD OS disk
- Windows 10 Enterprise for Virtual Desktop
- FSLogix attached containers user profile
- Attached storage for company share

**GPU Users (SKU: VDMS-SUBS-GPU-USER)**

A GPU user's session runs on a dedicated Session Host Virtual Machine (SHVM) that does not concurrently host any other user sessions. The total number of GPU SHVMs is equal to the total number of GPU users in the environment.

**Resources allocated per GPU user:**

- 8 GiB GPU RAM
- 25 GiB Storage

**GPU SHVM technical details:**

- Typically from the NVv3 and NVv4 families of Azure virtual machines.
- 128 GiB Standard HDD OS disk
- Windows 10 Enterprise for Virtual Desktop
- FSLogix attached containers user profile
- Attached storage for company share

## Other VDMS SKUs

### Business Servers (SKU: VDMS-AZURE-BUSINESS-VM)

The business server can be added to an environment to support applications and services.

**Each business server VM is allocated at least:**

- 8 vCPU cores
- 64 GiB RAM
- 128 GiB Standard SSD OS disk
- Windows Server 2012R2/2016/2019
- Typically from the Esv3, Eav4 and Easv4 families of Azure virtual machines.

### Additional Storage (SKU: VDMS-1TB-STORAGE-HPRSCLR)

The *Data Storage Layer* is the primary storage mechanism for the VDMS environment and runs on either Azure Files or Azure NetApp Files (ANF). The storage technology used is determined by the total VDMS users purchased. Additional capacity can be added in 1TiB increments.

User profiles, user data, company shares, application data and databases should all run from this storage service. It is best practice to avoid storing data on VM disks whenever possible.

Capacity is the sum of the per-user allocation (25 GiB/user) and additional TIBs storage purchased.

**Table 1. Data Storage Layer Type & Tier**

| Metric | Azure Files GPv2 | ANF Standard | ANF Premium |
|---|---|---|---|
| User Count | 10-49 | 50-249 | 250+ |
| Minimum size | 250 GiB | 4 TiB | 4 TiB |
| IOPS | Up to 1,000 | Up to 250/TiB | Up To 1,000/TiB |
| Throughput | Up to 60MiB/sec | Up to 16 MiB/sec/TiB | Up to 64 MiB/sec/TiB |

# Tutorials

## Installing applications on the session host virtual machine(s)

### Application Delivery Methodology

Users can access any applications that are installed the session host virtual machine (SHVM) where their user session is running.

Users are assigned to a pool of SHVMs ("host pool") based on their membership in a user group. Every SHVM in that host pool is based on the same VM Image, has the same applications and runs on the same VM resources. Each time a user connects, they are assigned to SHVM in their host pool with the fewest current user sessions.

By adding or removing applications from each SHVM in the host pool the VDMS administrator can control which applications VDMS users can access.

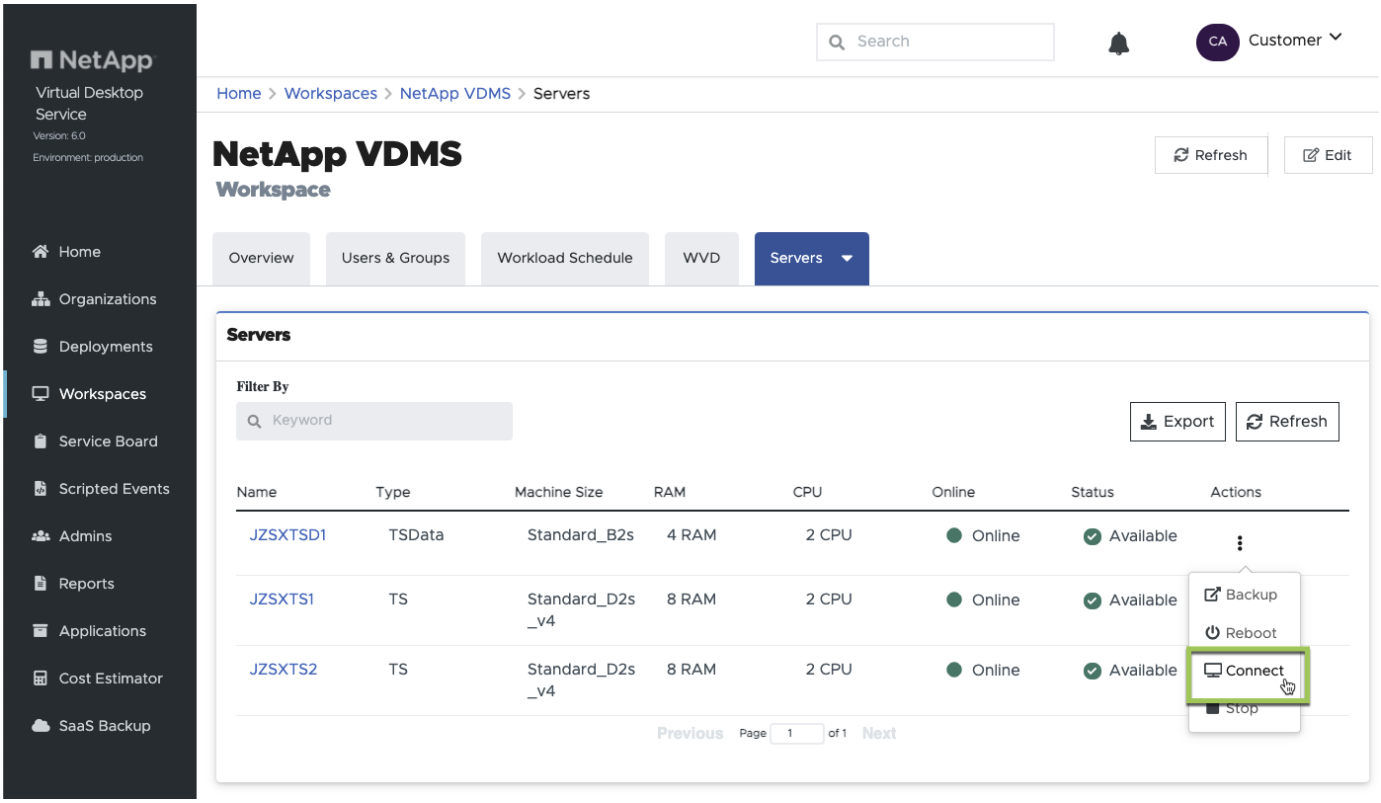
Adding (or removing) applications from each SHVM can be performed directly on each SHVM or to a single VM Image which in turn can be deployed to all SHVMs in the host pool.

This article covers directly installing applications on the SHVMs. VM Image management is covered in this article.

#### Manual Access

The VDMS management portal provides direct access to each VM via a just-in-time local admin account for all SHVMs and business servers. This access can be used to manually connect to each VM to manually install applications and make other configuration changes.

This functionality is found in Workspace > Servers > Actions > Connect




If domain admin credentials are required, VDMS privileged access management (PAM) functionality to generate domain admin credentials. Details can be found here.

### VDMS Automation

With the VDMS portal, the "Scripted Events" section includes functionality to remotely run code.

Within Scripted Events, the Repository tab contains "global" scripts that are published by NetApp. Custom scripts can be added using the "+ Add Script" button.

Within Scripted Events, the Activities tab contains the trigger that causes a script to run against a set of VMs. For VDMS, the "Manual" and "Scheduled" event types are best to push a script across the appropriate virtual machines.

Activities have many available triggers called "Event Types". For VDMS, the "Application Install" and "Application Uninstall" types do not apply. These are RDS-specific triggers and should not be used for VDMS since VDMS is a WVD-based service, and does to follow the design architecture of RDS.

### Other Automation Tools

Virtual machines in VDMS can be managed with 3rd party management tools. Application changes and other VM configuration changes can be applied via any compatible tools.

# Update and Deploy VM Images

## Application Delivery Methodology

Users can access any applications that are installed the session host virtual machine (SHVM) where their user session is running.

Users are assigned to a pool of SHVMs ("host pool") based on their membership in a user group. Every SHVM in that host pool is based on the same VM Image, has the same applications and runs on the same VM resources. Each time a user connects, they are assigned to SHVM in their host pool with the fewest current user sessions.

By adding or removing applications from each SHVM in the host pool the VDMS administrator can control which applications VDMS users can access.

Adding (or removing) applications from each SHVM can be performed directly on each SHVM or to a single VM Image which in turn can be deployed to all SHVMs in the host pool.

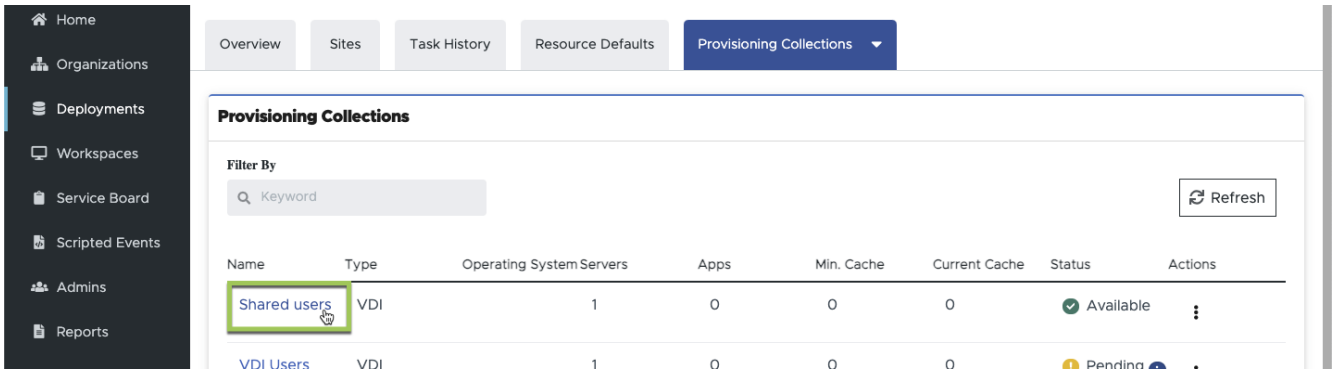
This article covers VM Image management. Directly installing applications on the SHVMs is covered in this article.

### Updating the VM Image

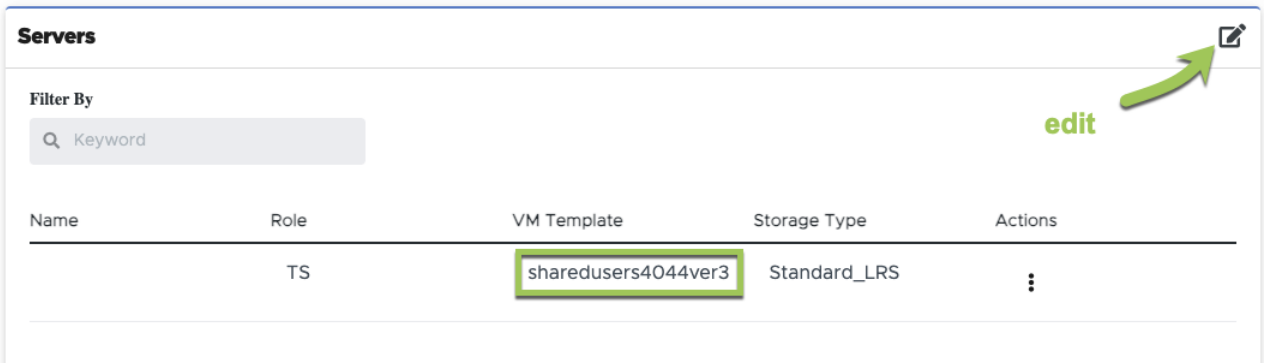
The recommended method for adding (or removing) applications to SHVM(s) is by editing the VM Image assigned to the host pool. Once the VM Image is customized and validated, the VDMS support team can deploy it to all SHVMs in the host pool upon request.

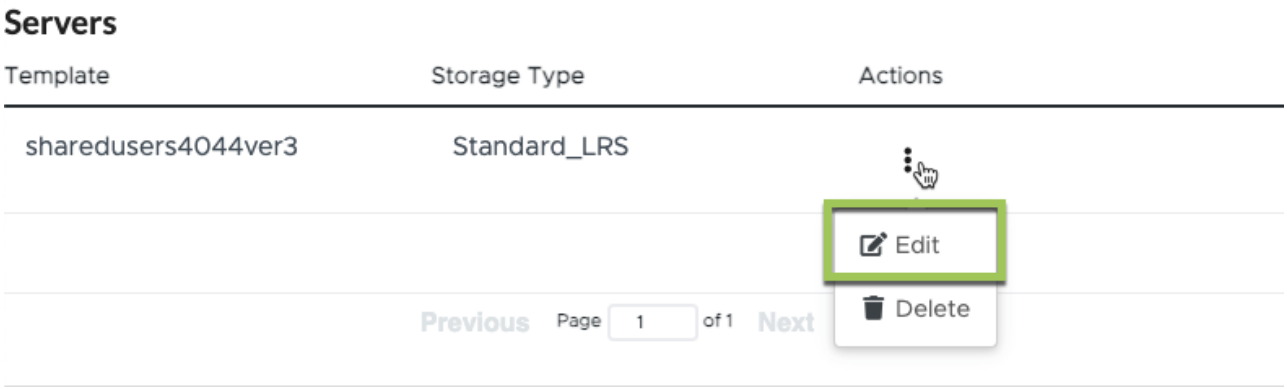
#### How to edit the VM image

1. Navigate "Provisioning Collections" within the deployment in the VDS portal
2. Click on the provisioning collection associated with the host pool you wish to update.

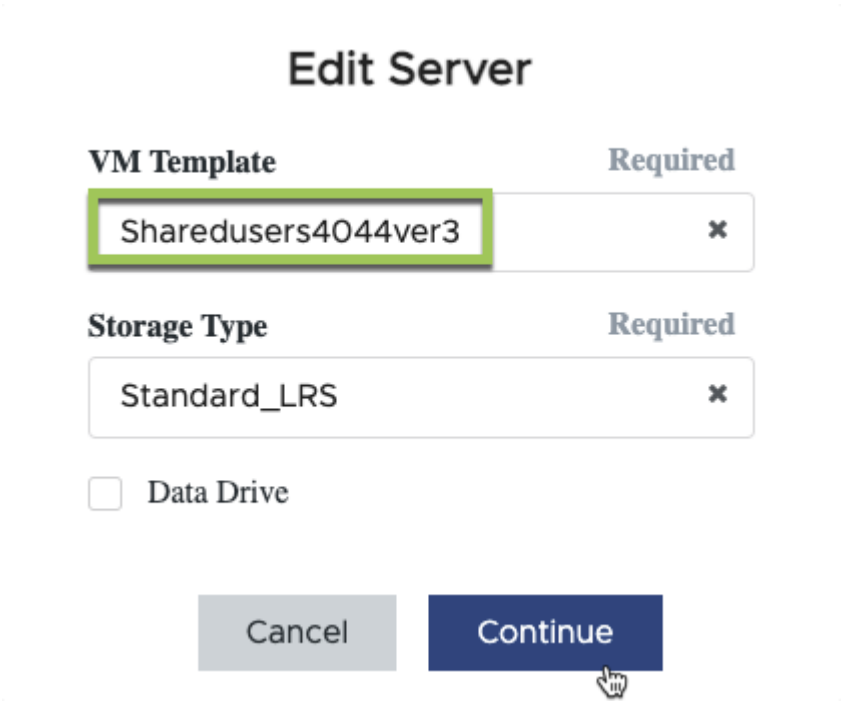



a. Make note of the "VM Template" name in the "Servers section.






3. Edit the Server template ensuring that the source template is the VM Template noted in step 2.a. above. Click "Continue"




**Don’t edit these settings:**
1. Type = VDI
2. Share Drive = empty
3. Minimum Cache = 0
4. Data Drive = Unchecked
5. Storage Type = Standard_LRS

1. The VDMS automation will now build a temporary VM in Azure, the machine name will be *CWT#*. Building this VM may take 25 minutes. Once the process completes the status will change to "Pending"
    a. Note, this VM will run until the customization process is complete so it is important to build, customize and validate the VM within a day or two.
2. Once the temporary VM is ready, you can log on to the VM by editing the Provisioning Collection and then clicking "Connect" on the server.
    a. When prompted for credentials, domain admin credentials can be generated by any VDMS admin with "PAM Approver" rights.

**How to deploy an updated VM image**

1. Once the VM image is validated, contact the VDMS support team to schedule an image refresh.
2. The team will build new session hosts based on the new image.
    a. If required, please coordinate time to test the new hosts before we redirect new users to the new hosts.
3. Once ready, the support team will redirect all new user sessions to the new hosts. We'll shut down the old hosts once no users are connected. These old VMs will remain in a deallocated state for warm failover but these VMs will be automatically purged after 7 days.

**Changing the SHVM(s) directly**

Changes can be made directly on the SHVM(s) manually or via any available automation tools. More information on this is found in this article.

When making changes directly to the SHVMs in a host pool it is critical that each SHVM remain configured in the same way or users may have inconsistent experiences as they connect to different SHVMs.

By default, individual SHVMs are not backed up because they typically don't have unique data and are based on a standardized VM image. If you're making customizations directly to the SHVMs, please contact support to get a backup policy applied to one of the SHVMs in the host pool.

**Sysprep Troubleshooting**

The VDMS image "Validate" function uses Microsoft's Sysprep utility. When validation fails, the most common culprit is a Sysprep failure. To troubleshoot failures, start in the Sysprep log file located on the CWT# VM in the path: C:\windows\system32\Sysprep\panther\setupact.log

# Assigning Users to App Groups

## User Assignment Methodology

Users are assigned to a session host virtual machine (SHVM) through AD security groups.

For each host pool, there is a linked user group on the "Users & Groups" tab within the workspace.

User groups are named with the workspace ID (a unique 3-4 digit code for each workspace), followed by the name of the host pool.

For example, the group "jzsx Shared Users" is linked to the Shared Users host pool in VDMS. All users added to "jzsx Shared Users" will be assigned access to the session hosts in the "Shared Users" host pool.

**To assign a user to their host pool**

1. Navigate to "Users & Groups" within the workspace
2. Users can be added to the group by editing the user list within the group.
3. Automation will automatically sync the members of the user group such that the user will be granted access to the appropriate host pool, app group and applications.

Users should only be assigned to one (and only one) app group. The type of host pool (Shared, VDI or GPU) must match the licensed SKUs purchased for VDMS. Misalignment of users and/or assignment to multiple app groups will cause resource contention issues and potentially impact their colleagues working in the environment.

# Generate Domain Admin Credentials in VDMS

## Privileged Access Management

VDMS admins can be given the "PAM Approver" role which enables the admin to grant PAM requests.

PAM requests will generate a domain level admin account to be used to authenticate on VDMS VMs when the just-in-time local admin credentials are not sufficient.

Any VDMS admin can submit a PAM request but only admins with the PAM Approver role can approve the requests. A PAM Approver can both request and approve their own request.

### Submit a PAM Request

**To submit a PAM request**

1. Navigate to your admin username in the upper right corner and click "Settings"
2. Select the "PAM Requests" tab
3. Click "+ Add"
    a. Select a duration, after which these credentials will expire
    b. Choose the deployment
    c. Enter an email address that the credentials can be provided. This can be any email address, allowing 3rd parties (e.g. a vendor) to be granted domain credentials.
    d. Enter a phone number that can receive text messages
    e. Enter any notes for the logs and for the PAM Approver to review.
4. Click "Add Request"

### Approve a PAM Request

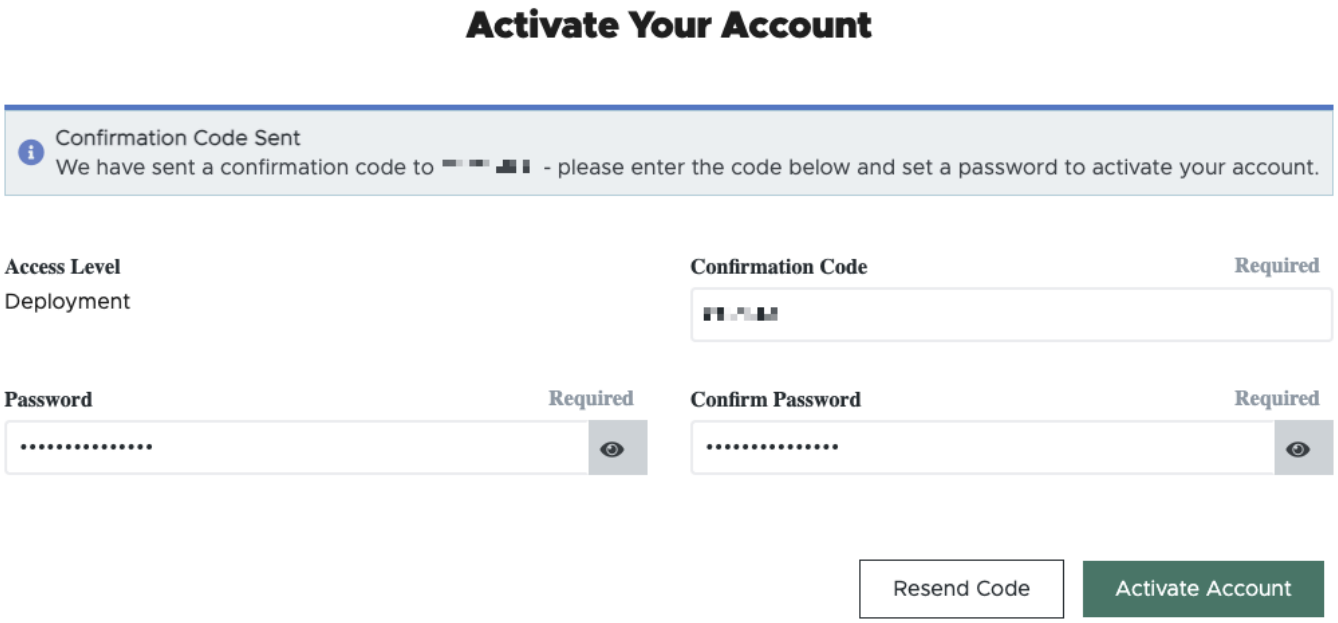
**To review and approve/reject a PAM request**

1. . Navigate to your admin username in the upper right corner and click "Settings"
2. Select the "PAM Requests" tab and click on the request
3. Review the request and click "Approve" or "Reject"
4. Enter any notes relevant to the approval/rejection decision

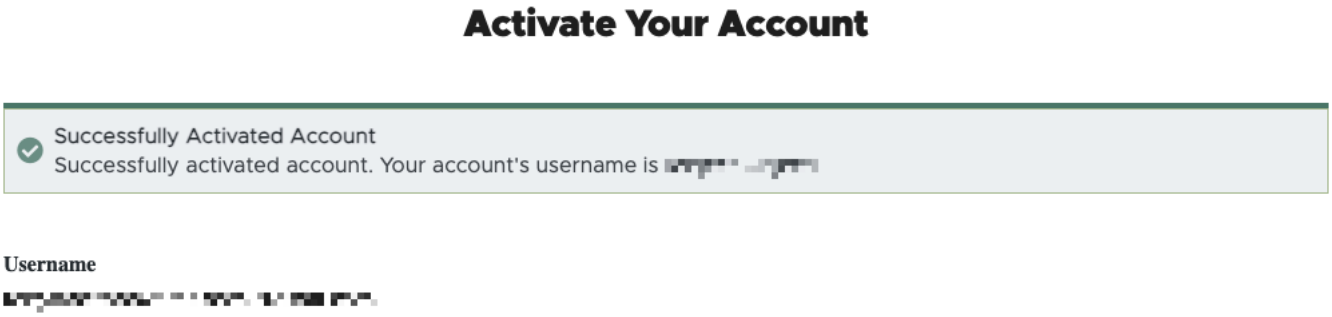
### Using PAM Generated Credentials

Once approved, the provided email address is sent a confirmation email to activate their credentials:


Following the "Activate Request" link will bring the user to the following page and send them a confirmation code via SMS. They will also be asked to set a secure password.




Upon successfully validating the account, the user receives a confirmation with their username.

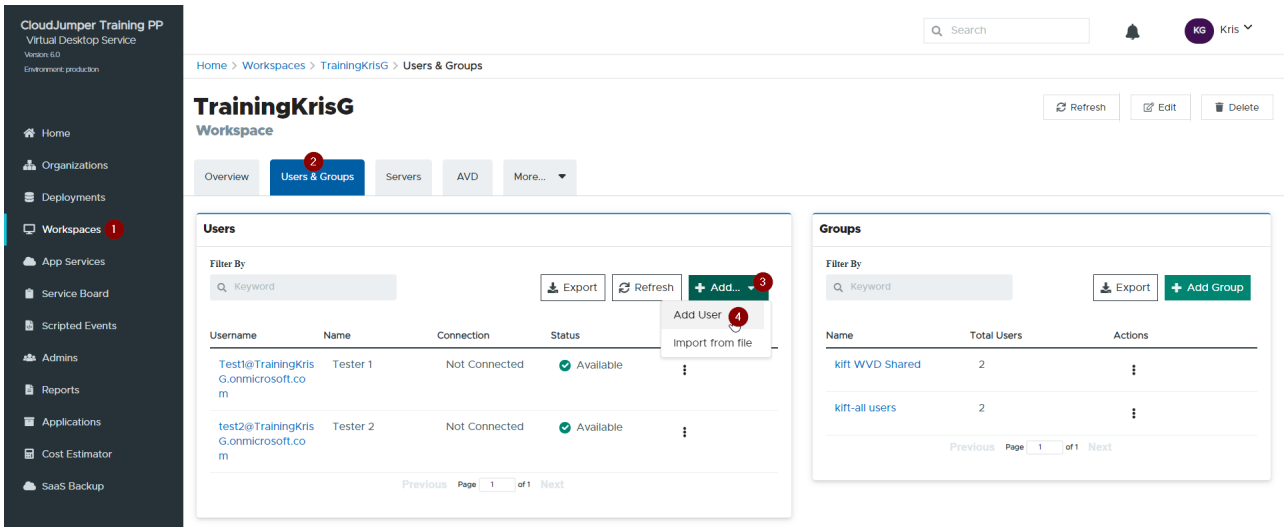



# Adding User Access

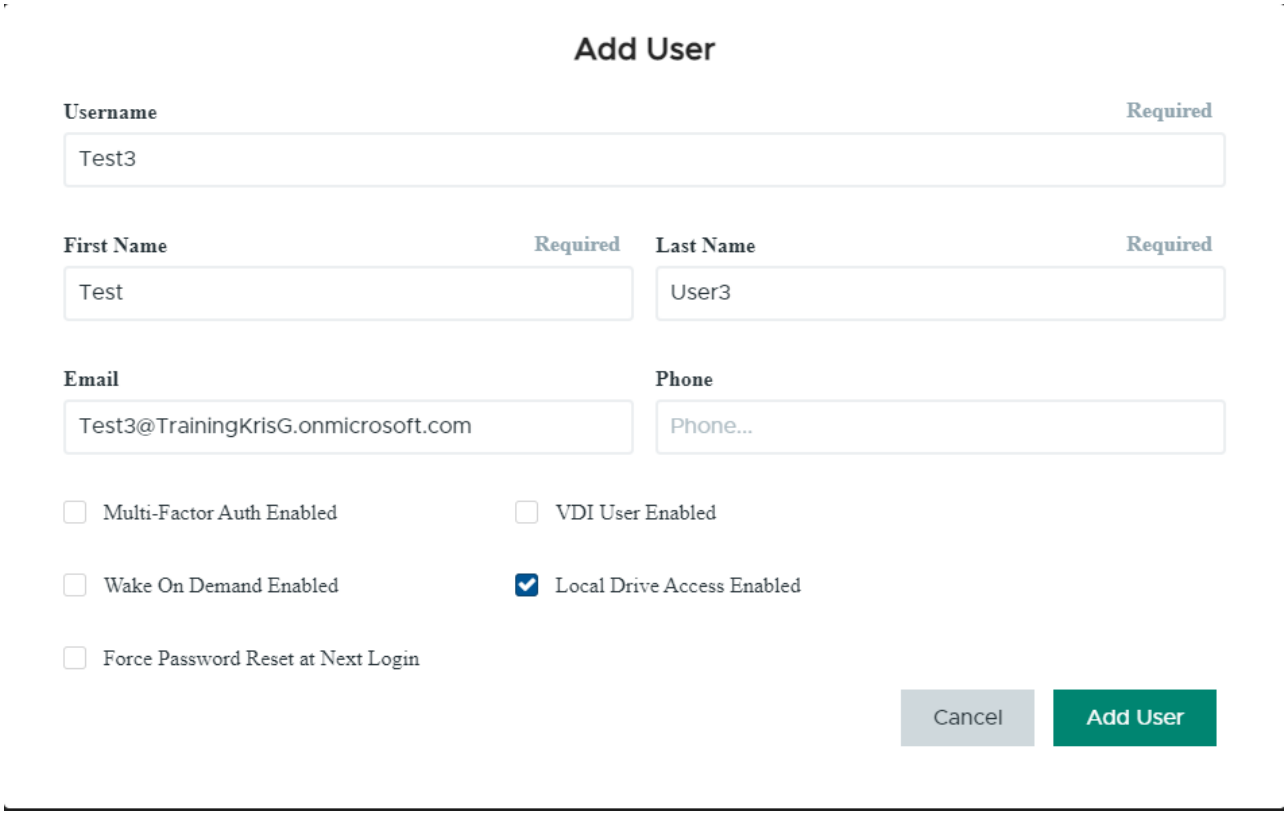
## New User Creation

**New Active Directory deployments (a new Active Directory domain was created for VDMS)**

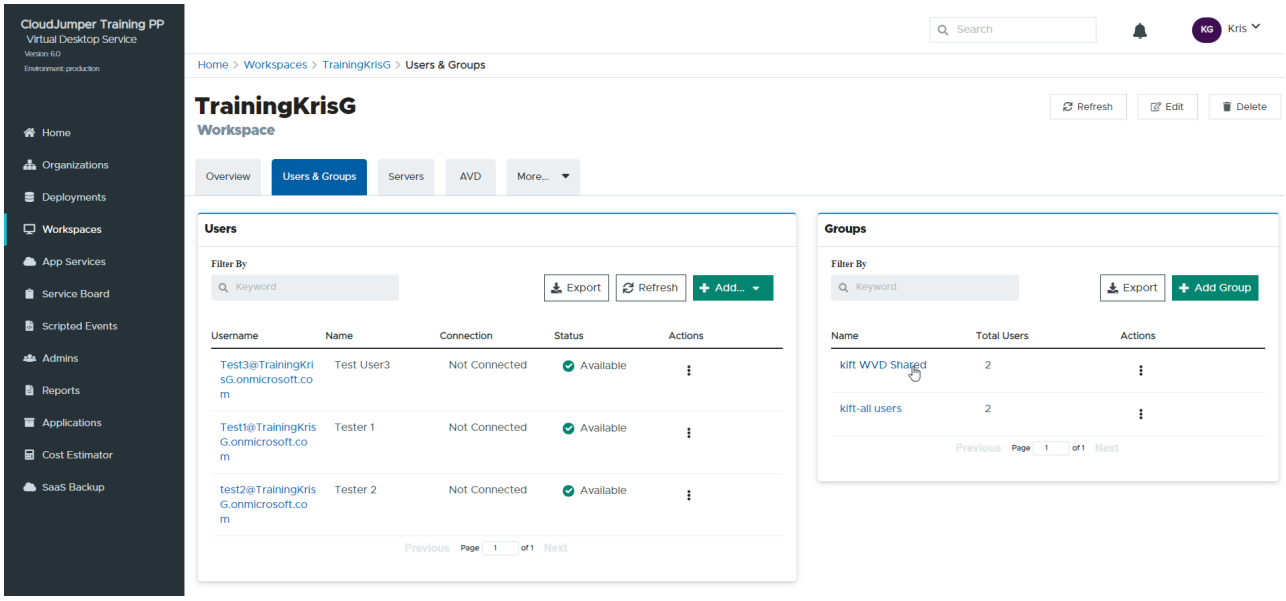
1. Create the user in VDS
    a. Navigate to the workspace, select the "Users & Groups" tab, click "Add", and select "Add User"



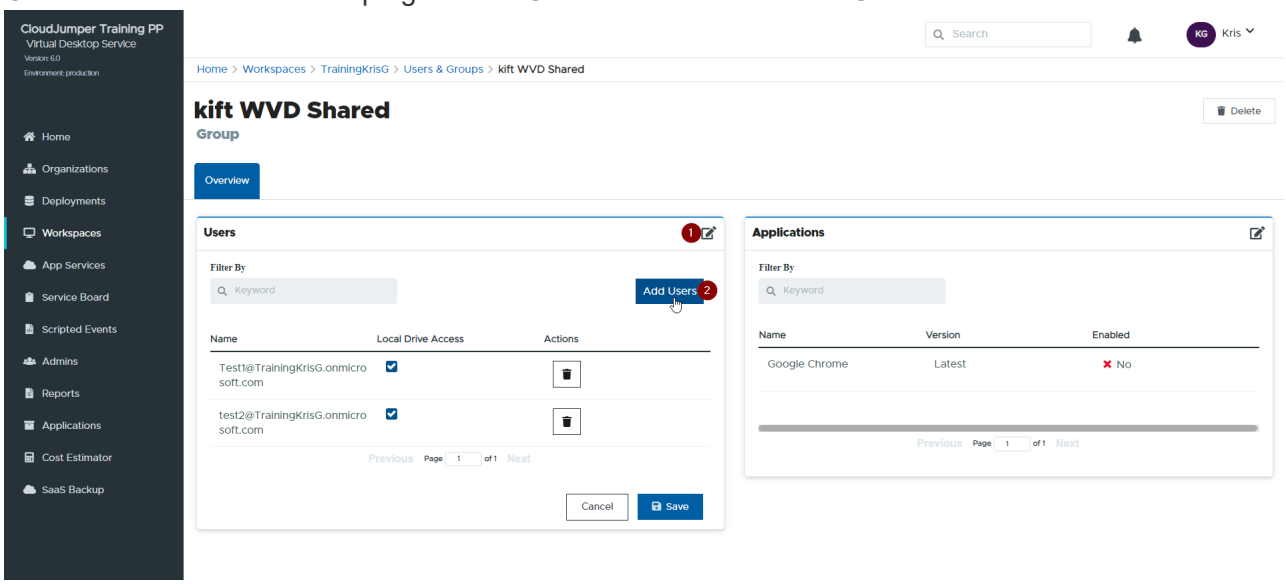

b. Fill in the user's information then click "Add User"



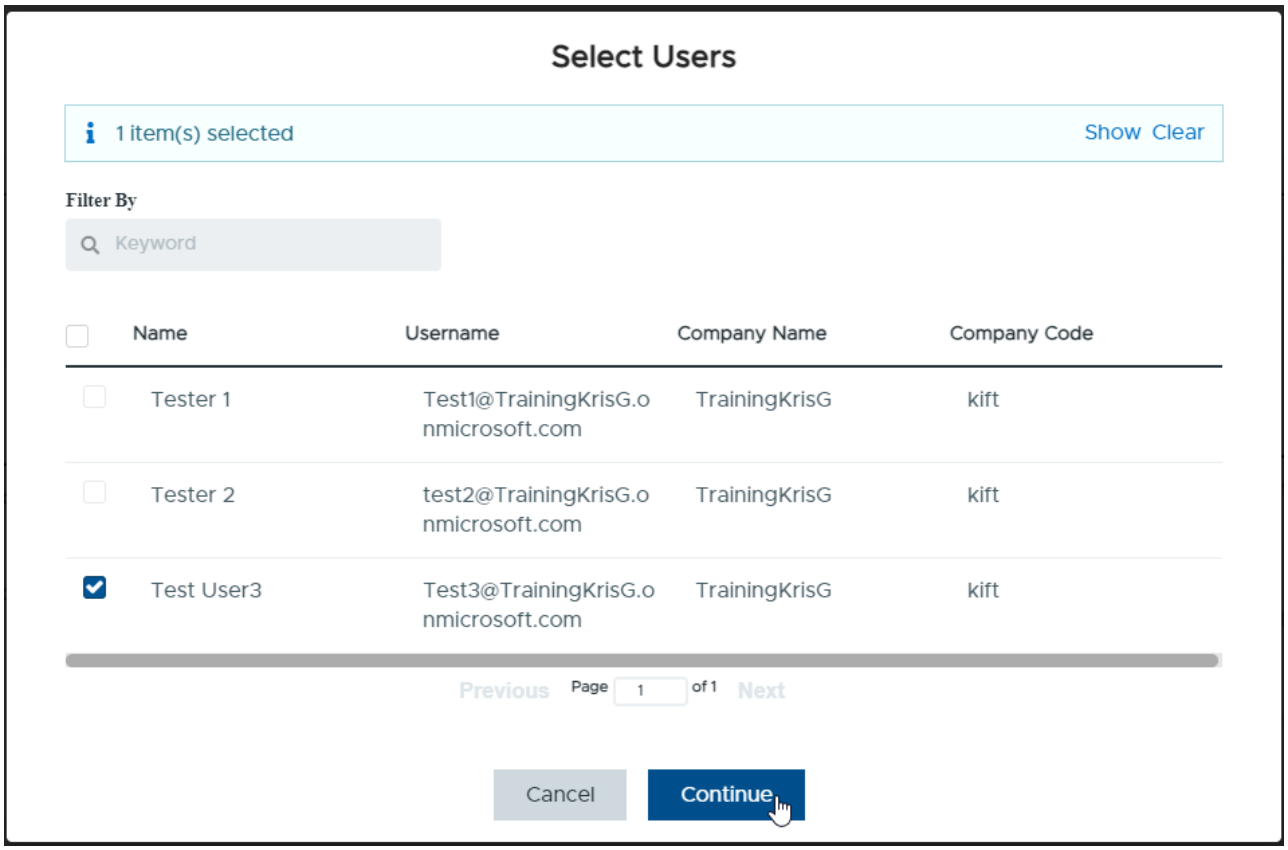

2. Notify NetApp of the additional user using one of the methods below
   a. Email support: VDSsupport@netapp.com
   b. Phone Support: 844.645.6789
   c. VDMS Support Portal
3. Assign the user to their host pool
   a. On the users and groups tab, click on the user group linked to the host pool. For example, the group "kift WVD Shared" is linked to the WVD Shared host pool in VDMS. All users added to "kift WVD Shared" will be assigned access to the session hosts in the "WVD Shared" host pool.




b. Click on the edit icon inthe top right of the Users box then click "Add Users"



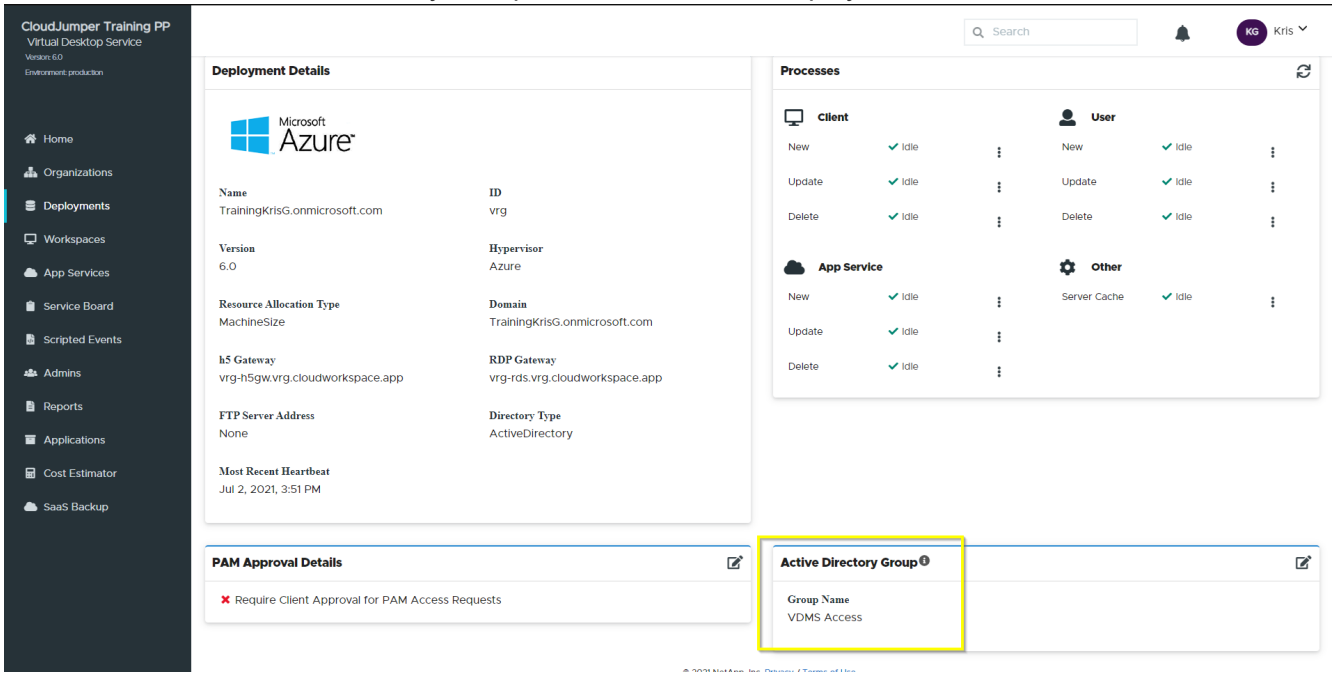

c. Check the box next to the user(s) to be added then click "Continue"




d. More detailed instructions can be found here

**Existing Active Directory deployments (VDMS is connecting to an existing Active Directory)**

1. Create the user in Active Directory as you normally would
2. Add the user to the Active Directory Group that is listed on the deployment



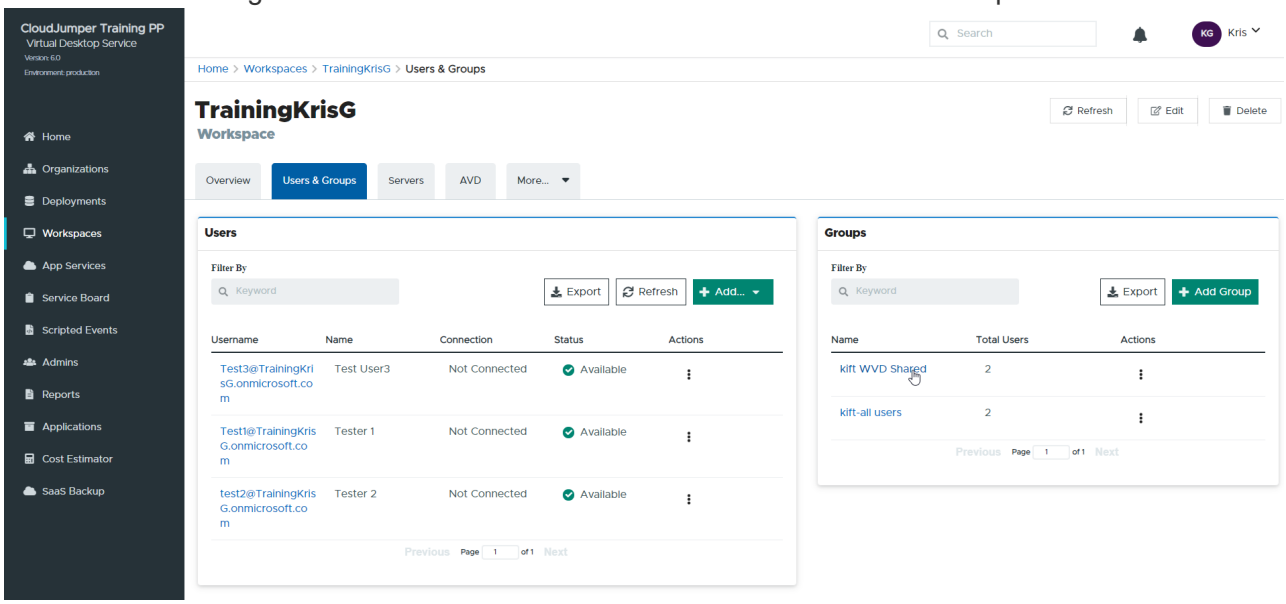

3. Enable cloudworkspace
4. Notify NetApp of the additional user using one of the methods below
   a. Email support: VDSsupport@netapp.com

b. Phone Support: 844.645.6789

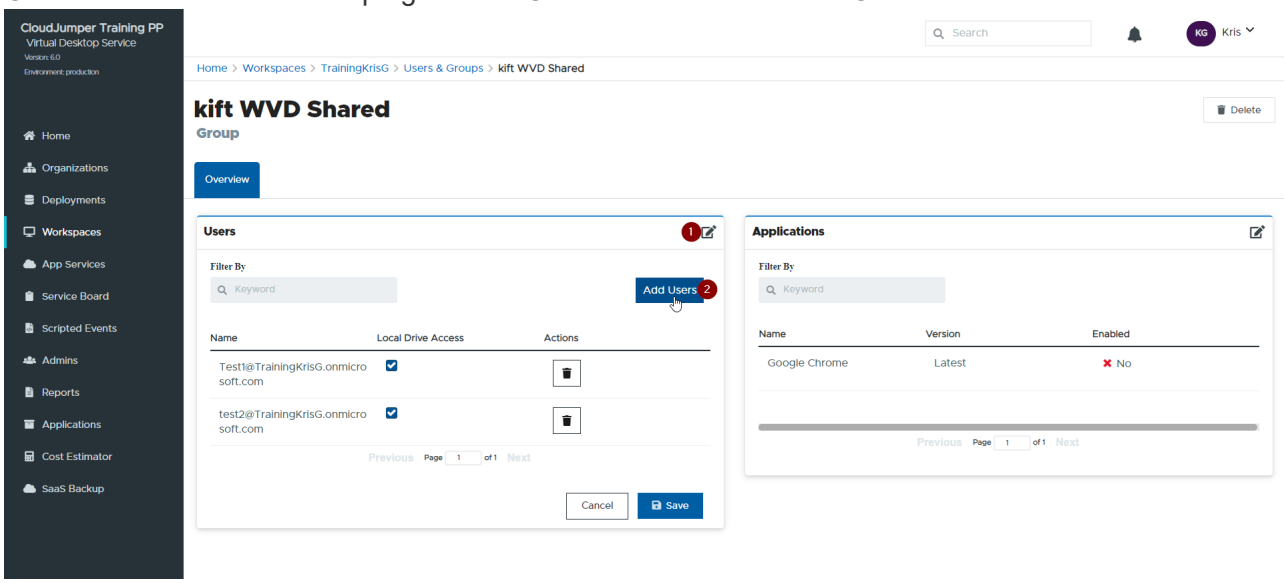
c. VDMS Support Portal

5. Assign the user to their host pool

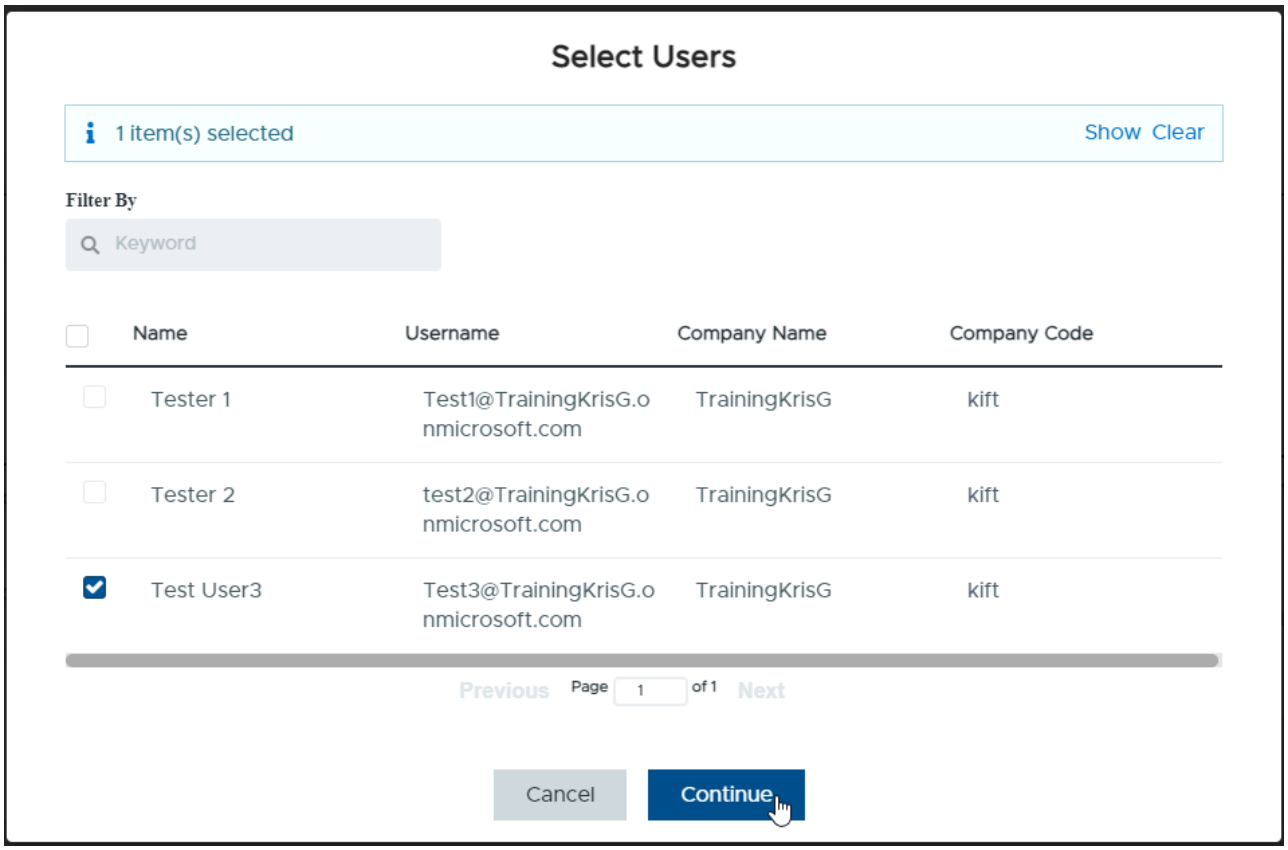
a. On the users and groups tab, click on the user group linked to the host pool. For example, the group "kift WVD Shared" is linked to the WVD Shared host pool in VDMS. All users added to "kift WVD Shared" will be assigned access to the session hosts in the "WVD Shared" host pool.




b. Click on the edit icon inthe top right of the Users box then click "Add Users"




c. Check the box next to the user(s) to be added then click "Continue"




d. More detailed instructions can be found here

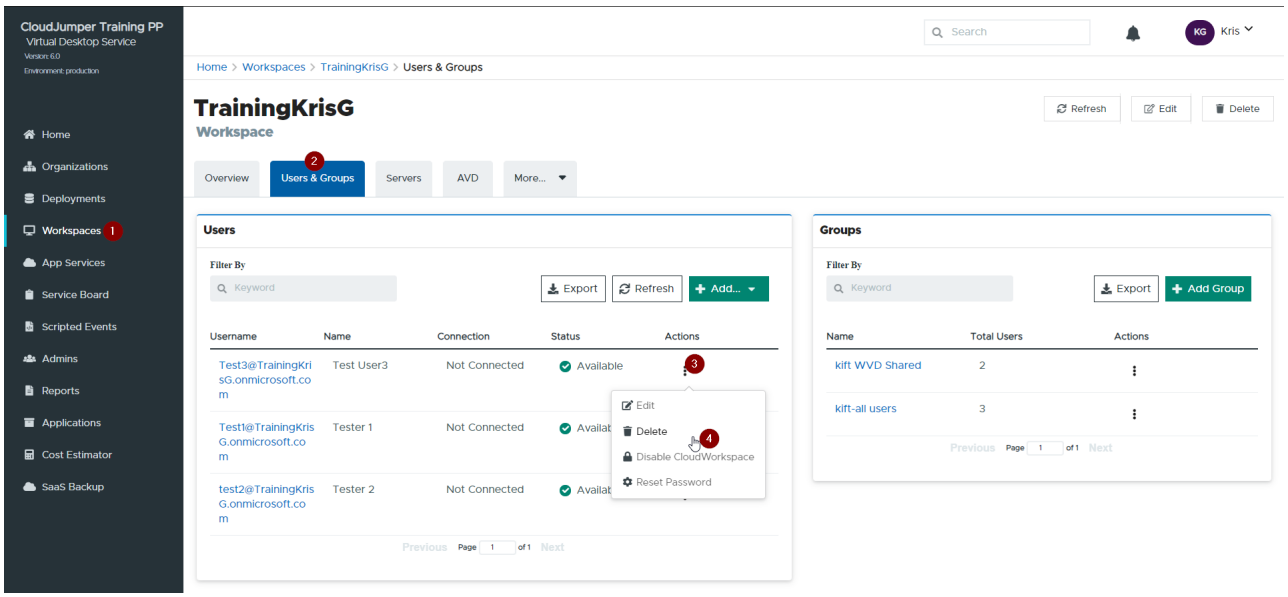
# Removing User Access

## Removing a User

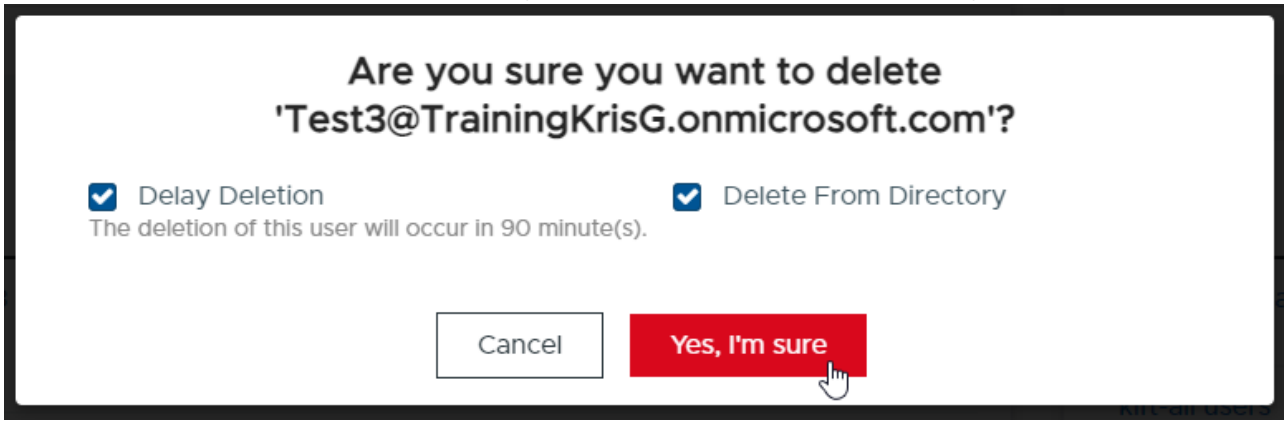
**New Active Directory deployments (a new Active Directory domain was created for VDMS)**

1. Delete the user in VDMS

   a. Navigate to the workspace, select the "Users & Groups" tab, click the action dots next to the user to be deleted, then click "Delete"



b. A pop up pwill appear with options to Delay Deletion and Delete From Directory




i. The Delay Deletion option will wait 90 minutes before deleting the user, which allows for the process to be cancelled. It is recommended to check this box.

ii. The Delete From Directory option will delete the Active Directory user account. This box should be checked.

2. Notify NetApp of the user removal using one of the methods below

a. Email support: VDSsupport@netapp.com

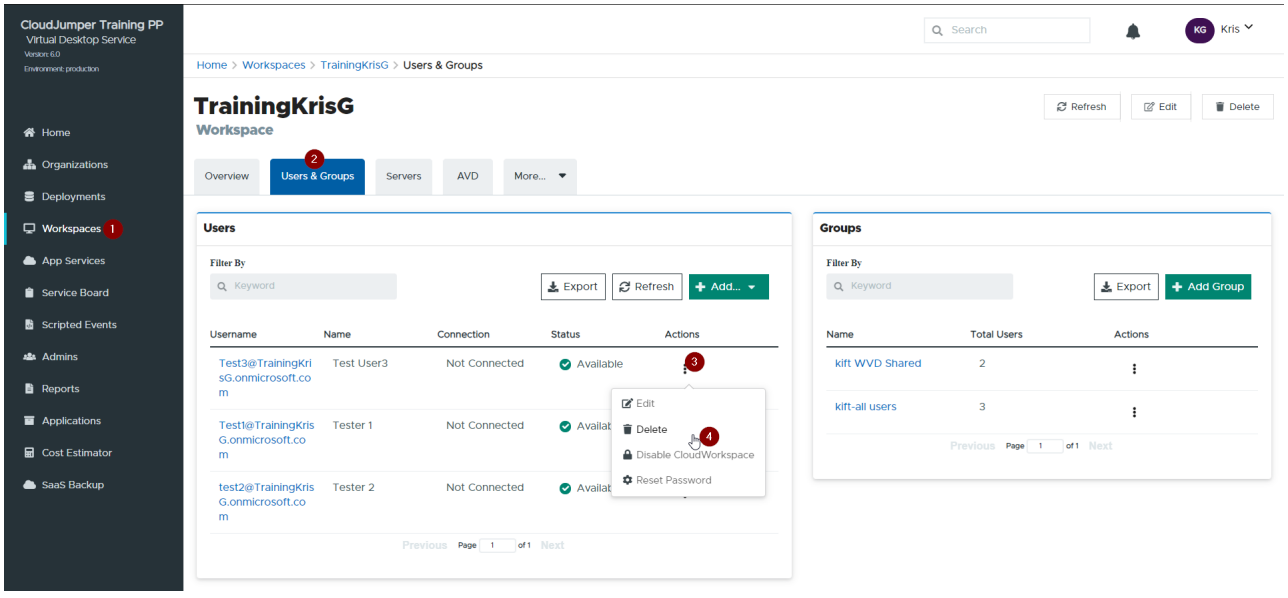
b. Phone Support: 844.645.6789

c. VDMS Support Portal

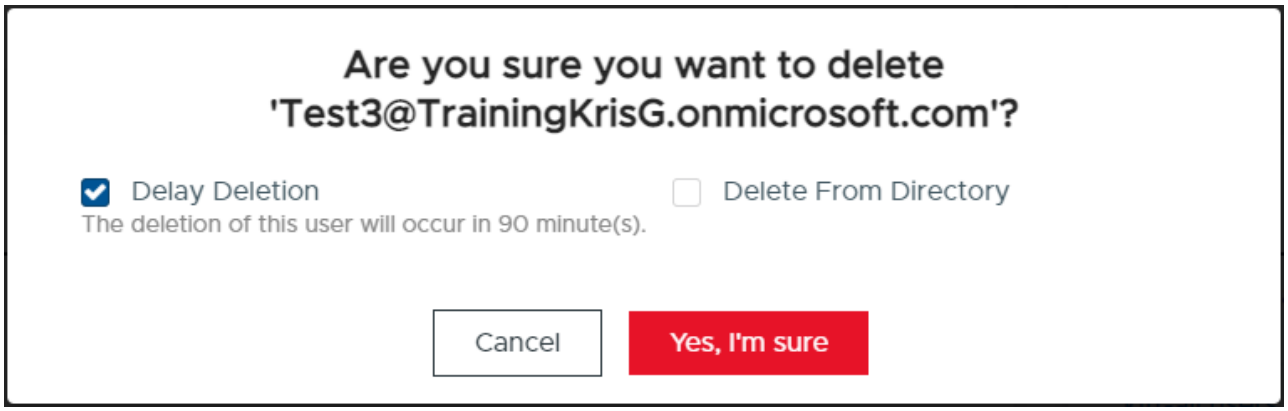
**Existing Active Directory deployments (VDMS is connecting to an existing Active Directory)**

1. Delete the user in VDMS

a. Navigate to the workspace, select the "Users & Groups" tab, click the action dots next to the user to be deleted, then click "Delete"




b. A pop up pwill appear with options to Delay Deletion and Delete From Directory




i. The Delay Deletion option will wait 90 minutes before deleting the user, which allows for the process to be cancelled. It is recommended to check this box.

ii. The Delete From Directory option will delete the Active Directory user account. It is recommended this box is NOT checked, and your organizations user account deletion process be followed to delete the account from Active Directory.

2. Notify NetApp of the user removal using one of the methods below
   a. Email support: VDSsupport@netapp.com
   b. Phone Support: 844.645.6789
   c. VDMS Support Portal

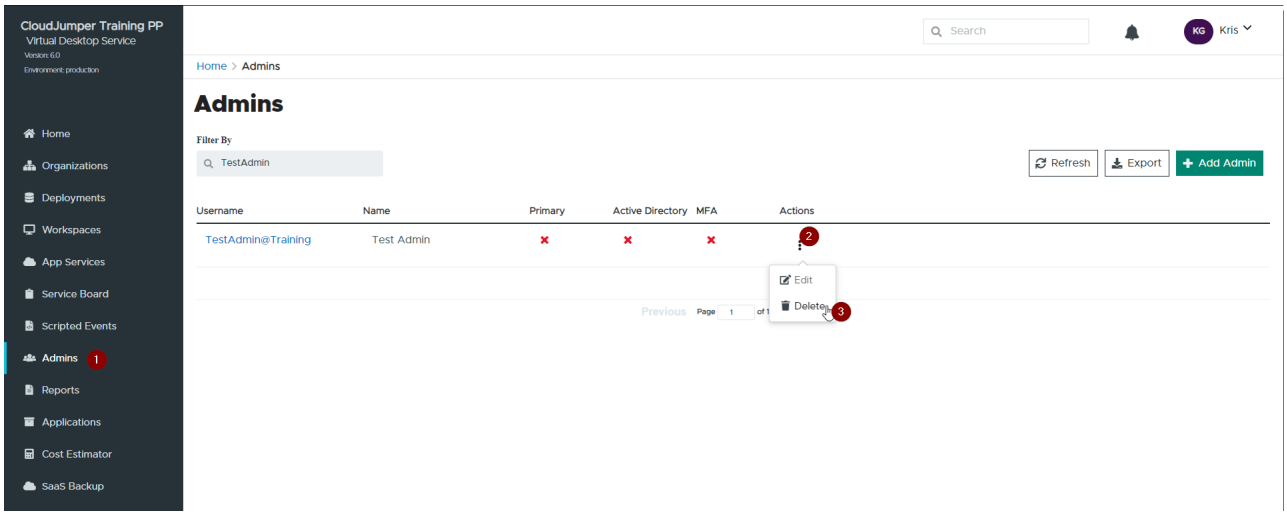
# Adding and Removing Admins in VDMS

## Adding Admins in VDMS

- This process is handled by NetApp
- Contact NetApp VDMS support using one of the methods below:
  1. Email support: VDSsupport@netapp.com
  2. Phone Support: 844.645.6789
  3. VDMS Support Portal
- Please include the following for the new admin account:
  1. Partner code
  2. First and last name
  3. Email address
  4. If any permissions differ from the default set that are outlined in the admin permissions

## Removing Admins in VDMS

- This process is handled by partners
  1. Navigate to the "Admins" tab
  2. Click the Action dots to the right of the admin you would like to remove
  3. Click "Delete"
  4. A confirmation box will appear; click on "Yes, I'm sure"




- If you have any questions, contact NetApp VDMS support using one of the methods below:
  1. Email support: VDSsupport@netapp.com
  2. Phone Support: 844.645.6789
  3. VDMS Support Portal

# VDMS FAQ’s

## VDS Admin Permissions

### Admin Permissions Overview

VDMS admins have limited access to the VDS administration portal. Because VDMS is a co-managed solution there are permission sets that are not enabled for VDMS admins. These actions are reserved for the NetApp support team. If there are actions needed that can not be performed due to permission limitations, please contact support for assistance.

### Account Type Settings

Within the VDMS admin account, the following settings are default.

| Type | Default Value | Notes |
|---|---|---|
| Tech Account | False | Can be changed upon request to NetApp Support.<br><br>When enabled, admin is prompted for credentials when connecting to any VM via the VDS portal.<br><br>When disabled, admin is automatically authenticated (with auto-generated local admin account) when connecting to any tenant VM via the VDS portal. Admins are still prompted for credentials when connecting to any platform server VMs. |
| PAM Approver | True | Can be changed upon request to NetApp Support.<br><br>All customer’s must have at least one admin account enabled as PAM Approver. |
| User Support | False | This feature does not apply to VDMS. |
| Shadow User | True | Can be changed upon request to NetApp Support.<br><br>When enabled, the admin is able to connect to an end user’s session and see what they see for providing end user support. |

| Type | Default Value | Notes |
| --- | --- | --- |
| MFA Enabled | True | Requires that the admin's access to the VDMS administration portal be secured using built-in MFA. SMS and/or email methods are supported. |

## Admin Account Permissions

Within the VDMS admin account, the following permissions are default.

| Module | View | Edit | Delete | Add | Notes |
| --- | --- | --- | --- | --- | --- |
| Admin | On | Off | On | Off | Adding admin accounts and/or changing admin permissions is handled by NetApp Support. |
| App Services | Off | Off | Off | Off | The App Services feature set is not a supported feature in VDMS. |
| Applications | Off | Off | Off | Off | The Applications feature-set in VDS is RDS-specific. VDMS is a WVD-based service and application management is not handled with this function. See update and deploy images for details on application delivery for VDMS. |
| Audits | On | On | On | On | |
| Clients | On | On | Off | Off | Client creation/removal is handled by NetApp Support. |
| Deployments | On | On | Off | Off | Deployment creation/removal is handled by NetApp Support. |

| Module | View | Edit | Delete | Add | Notes |
|---|---|---|---|---|---|
| Firewall Rules | On | On | On | On | |
| Folders | On | On | On | On | |
| Groups | On | On | Off | On | Deleting user groups is handled by NetApp Support. Certain user groups are required |
| Partners | On | Off | Off | Off | The Partners feature set is not a supported feature in VDMS. View permissions required to display tenant lists. |
| Provisioning Templates | On | On | Off | Off | Image creation/removal is handled by NetApp Support. |
| Reports | On | On | On | On | |
| Resources | On | Off | Off | Off | Resource settings are handled by NetApp Support. |
| Scripted Events | On | On | On | On | |
| Servers | On | On | Off | Off | Server creation/removal settings are handled by NetApp Support. |
| Service Board | On | On | On | On | |
| Settings | On | On | On | On | |
| Users | On | On | On | On | |
| Workspaces | On | On | Off | Off | Workspace creation/removal is handled by NetApp Support. |