



Management

Virtual Desktop Service

NetApp
September 12, 2021

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Management.Deployments.provisioning_collections.html on September 12, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Management	1
Deployments	1
Applications	12
Scripted Events	25
Command Center.....	30
Resource Optimization.....	35
User Administration	42
System Administration	65

Management

Deployments

Provisioning Collections

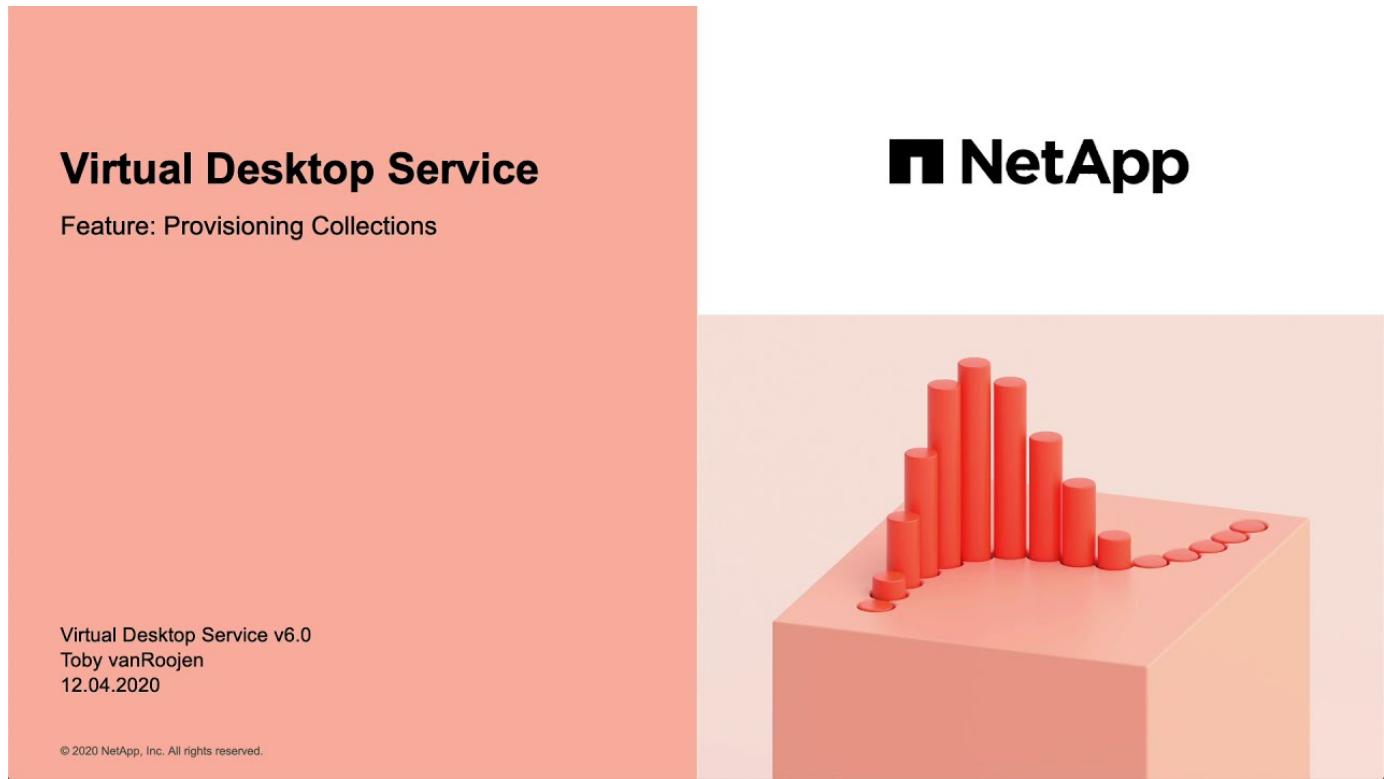
Overview

Provisioning Collections is a function of VDS related to the creation and management of VM images.

At a high level, the Provisioning Collection workflow is as follows:

1. A temporary VM (e.g. "CWT1") is built based on an existing image (either a stock image or a previously saved Provisioning Collection).
2. The VDS Administrator customizes the temporary VM to match their requirements using [Scripted Events](#), [Connect to Server](#) and/or 3rd party management tools.
3. Once customized, the VDS Admin click **Validate** and triggers a validation process that automates finalizing the image, running SysPrep, deleting the temporary VM and making the image available for deployment throughout VDS.

[Video Demo - Managing VM images for VDI Session Hosts](#)



Provisioning Collection Types

There are two distinct types of collection with specific use cases, **Shared** and **VDI**.

Shared

The **Shared** type is a collection of VM images(s) designed to deploy an entire environment with multiple,

distinct VM images and VM roles.

VDI

The **VDI** type is a single VM image designed to be used and reused to deploy multiple identical VMs, typically used for hosting user sessions. For all types of AVD session hosts, the **VDI** type should be selected, even for hosts that run multiple sessions per VM.

Creating a new Provisioning Collection

Provisioning Collections are found in the VDS interface within each deployment, under the **Provisioning Collections** sub-tab.



To create a new collection

1. Click the **+ Add Collection** button.
2. Complete the following fields:
 - a. **Name**
 - b. **Description**(Optional)
 - c. **Type** - Shared or VDI
 - d. **Operating System**
 - e. **Share Drive** - If this VM will be used to host users profiles or company share data, pick the drive letter on which it will be hosted. If not, leave as "C"
 - f. **Minimum Cache** - If you and VDS to create VMs to hold for instant deployment, specify the minimum number of cached VMs that should be maintained. If deploying new VMs can wait for as long as it takes the hypervisor to build a VM, this can be set to "0" to save costs.
 - g. **Add Servers**
 - i. **Role** (If "Shared" type is selected)
 - A. **TS** - This VM will act only as a session host
 - B. **Data** - This VM will not host any user sessions
 - C. **TSDATA** - This VM will be both the session host and the storage host (Maximum: one TSDATA per workspace)
 - ii. **VM Template** - Select from the available list, both stock hypervisor images and previously saved Provisioning Collections are available to select.
 - A. NOTE: Windows 7 images from the Azure Marketplace do not have PowerShell Remoting enabled. To use a Windows 7 image, you'll need to provide a custom image in your shared image gallery with PowerShell Remoting enabled.
 - B. NOTE: By using an existing Provisioning Collection you can update and re-deploy existing images as part of a planned image upgrade process.
 - iii. **Storage Type** - Select the speed of the OS disk considering cost and performance
 - iv. **Data Drive** - Optionally enable a 2nd disk attached to this image, typically for the data storage layer referenced above in 2.e.

- A. **Data Drive Type** - Select the speed of the 2nd (data) disk considering cost and performance
- B. **Data Drive Size (GB)** - Define the size of the 2nd (data) disk considering capacity, cost and performance
- h. **Add Applications** - Select any application from the Application Library that will be (1) installed on this image and (2) managed by VDS application entitlement. (This is only applicable to RDS deployments. It should remain empty for AVD workspaces)

Customizing the Temporary VM

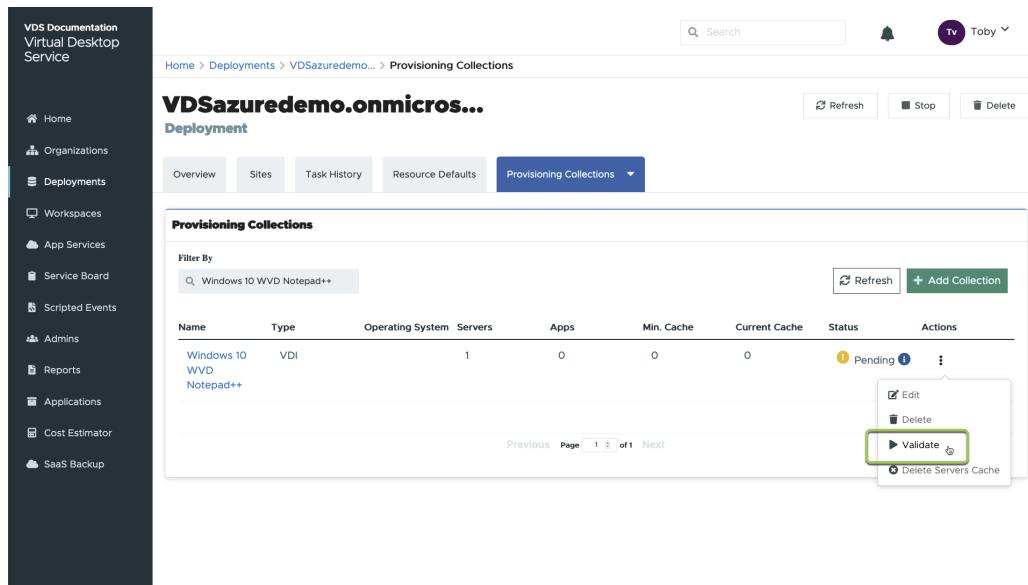
VDS includes functionality that will allow remove VM access from within the VDS web interface. By default a local Windows admin account is created with a rotating password and passed through to the VM allowing the VDS admin local admin access without needing to know local admin credentials.

 The Connect to Server function has an alternative setting where the VDS admin will be prompted for credentials with each connection. This setting can be enabled/disabled by editing the VDS admin account from within the "Admin" section of VDS. The functionality is called *Tech Account* and checking the box will require credential to be entered when using Connect to Server, unchecking this box will enable the automatic injection of local Windows admin credentials at each connection.

The VDS Admin simply needs to connect to the temporary VM using Connect to Server or another process and make the changes required to meet their requirements.

Validating the Collection

Once customization is complete, the VDS Admin can close the image and SysPrep it by clicking **Validate** from the Actions icon.



Name	Type	Operating System	Servers	Apps	Min. Cache	Current Cache	Status	Actions
Windows 10 WVD Notepad++	VDI		1	0	0	0	Pending	Edit Delete Validate Delete Servers Cache

Using the Collection

After validation has completed, the Status of the Provisioning Collection will change to **Available**. From within the Provisioning Collection the VDS Admin can identify the **VM Template** name which is used to identify this provisioning collection throughout VDS.

Name	Role	VM Template	Storage Type	Actions
TS		windows10e vdw13500ve r1	StandardSSD_LRS	:

New Server

From the Workspace > Servers page, a new server can be created and the dialog box will prompt for the VM Template. The template name from above will be found on this list:



VDS provides for an easy way to update session hosts in an RDS environment by using Provisioning Collections and the **Add Server** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations. For a detailed workflow on this process, see the [RDS Session Host Update Process](#) section below.

New AVD Host Pool

From the Workspace > AVD > Host Pools page, new AVD Host Pool can be created by clicking **+ Add Host Pool** and the dialog box will prompt for the VM Template. The template name from above will be found on this list:

Add Host Pool

Basic Info

Name	Required	Friendly Name
Name...		Friendly Name...
Site	Required	Workspace
Select a site...		Select a site first
Host Pool Type	Required	Custom Profile Path
Select a host pool type...		Custom Profile Path...

Validation Environment

Included Session Hosts

OS Disk Type
 Ephemeral Persistent

VM Template	Required	Machine Size Type	Required
windows10	x	Select machine size type...	
Windows10EVD3497ver1			
Windows10EVDwi3500ver1			

Number of Instances
1

Cancel **Save**

New AVD Session Host(s)

From the Workspaces > AVD > Host Pool > Session Hosts page, new AVD session host(s) can be created by clicking **+ Add Session Host** and the dialog box will prompt for the VM Template. The template name from above will be found on this list:

Shared WVD Pool

Host Pool

Session Hosts

Add Session Host

OS Disk Type
 Ephemeral Persistent

VM Template	Required	Machine Size Type	Required
Windows10	x	Standard_E2as_v4	x
Windows10EVD3497ver1			
Windows10EVDwi3500ver1			

Number of Instances
1

Cancel **Save**

VDS provides for an easy way to update session hosts in a AVD Host Pool by using Provisioning Collections and the **Add Session Host** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations. For a detailed workflow on this process, see the [AVD Session Host Update Process](#) section below.



New Workspace

From the Workspaces page, a new workspace can be created by clicking **+ New Workspace** and the dialog box will prompt for the Provisioning Collection. The Shared Provisioning Collection name will be found on this list.

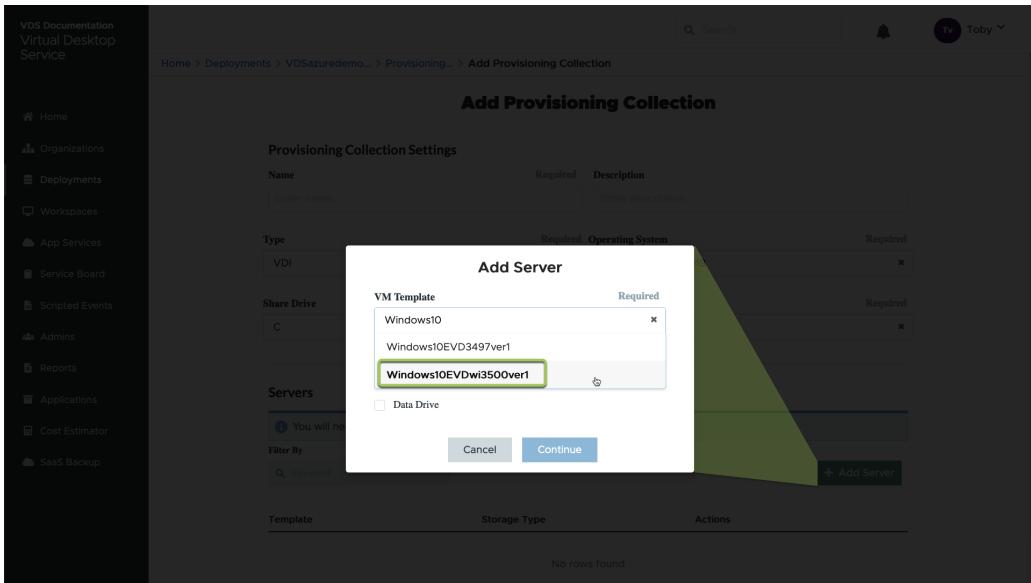
The screenshot shows the 'Add Workspace' dialog box with the 'Configure' tab selected. The top navigation bar includes a search bar, a bell icon, and a user profile for 'Toby'. The main form fields are as follows:

- Is this a new client?**: A radio button group where 'Yes' is selected.
- Company Name**: Omega Fuel
- Login Identifier**: @omegafuel
- Notification Email**: notify@omegafuel.abc
- Phone Number**: 5555555555
- Country**: United States
- Address 1**: 555 Main St
- Address 2**: Address 2...
- City**: Olympia
- State**: Washington
- Zip Code**: 98501
- Website**: Website...
- Internal Customer Number**: Customer number...
- Provisioning Info**
 - Deployment**: VDSGCPDemo (kxx)
 - Operating System**: Windows Server 2019
 - Provisioning Collection**: Default PC
 - Default PC** (highlighted with a green box)
 - Application Settings**
 - Enable Remote App
 - Enable App Locker
 - Enable Application Usage Tracking
- Device Settings**
 - Disable Printing Access
 - Enable User Profile Disk
 - Enable User Workspace Data Storage
 - Permit Access to Task Manager
- Security Settings**
 - Require Complex User Password
 - File Auditing Enabled
 - Migration Mode Enabled
 - Enable MFA for All Users

At the bottom are 'Cancel' and 'Next' buttons.

New Provisioning Collection

From the Deployment > Provisioning Collection page, a new Provisioning Collection can be created by clicking **+ Add Collection**. When adding servers to this collection the dialog box will prompt for the VM Template. The template name from above will be found on this list:



Addendum 1 - RDS Session Hosts

RDS Session Host Update Process

VDS provides for an easy way to update session hosts in a RDS environment by using Provisioning Collections and the **Add Server** functionality. This process can be done without impacting end users and repeated over and over with subsequent image updates, building on previous image iterations.

The RDS Session Host update process is as follows:

1. Build a new VDI Provisioning Collection, customize and validate the collection per the instructions above.
 - a. Generally this Provisioning Collection will be built on the previous VM Template, emulating an "Open, Save As" process.
2. Once the Provisioning Collection has validated, navigate to the *Workspace > Servers* page, click **+ Add Server**

3. Select **TS** as the **Server Role**
4. Select the latest **VM Template**. Make the appropriate **Machine Size** and **Storage Type** selections based on your requirements. Leave **Data Drive** unchecked.
5. Repeat this for the total number of Session Hosts required for the environment.
6. Click **Add Server**, the session hosts will build based on the selected VM Template and starting coming online in as soon as 10-15 minutes (depending on the hypervisor).

- a. Note that the Session Hosts currently in the environment will ultimately be decommissioned after these new host come online. Plan to build enough new hosts to be sufficient to support the entire workload in this environment.
7. When a new host comes online, the default setting is to stay in **Disallow New Sessions**. For each session host, the **Allow New Sessions** toggle can be used to manage which hosts can receive new user sessions. This setting is accessed by editing the settings of each individual session host server. Once sufficient new hosts have been built and functionality has been confirmed, this setting can be managed on both the new and old hosts to route all new sessions to the new hosts. The old hosts, with **Allow New Sessions** set to **disabled**, can continue to run and host existing user sessions.

The screenshot shows the 'Server Details' page for '5Z5WTS8'. The 'Connections' section contains a checkbox labeled 'Allow New Connections' which is checked and highlighted with a green border. The 'Save' button is visible at the bottom right of the modal.

8. As users log off of the old host(s), and with no new user sessions joining the old host(s), the old host(s) where **Sessions = 0** can be deleted by clicking the **Actions** icon and selecting **delete**.

The screenshot shows the 'Servers' list in the Azure WVD workspace. A context menu is open over the row for '5Z5WTSS', with the 'Delete' option highlighted with a green border.

Addendum 2 - AVD Session Hosts

AVD Session Host Update Process

VDS provides for an easy way to update session hosts in a AVD Host Pool by using Provisioning Collections and the **Add Session Host** functionality. This process can be done without impacting end users and repeated

over and over with subsequent image updates, building on previous image iterations.

The AVD Session Host update process is as follows:

1. Build a new VDI Provisioning Collection, customize and validate the collection per the instructions above.
 - a. Generally this Provisioning Collection will be built on the previous VM Template, emulating an "Open, Save As" process.
2. Once the Provisioning Collection has validated, navigate to the *Workspace > AVD > Host Pools* page and click the name of the Host Pool
3. From within the *Host Pool > Session Hosts* page, click **+ Add Session Host**

The screenshot shows the 'Add Session Host' dialog box. At the top, it says 'Add Session Host'. Below that, under 'OS Disk Type', there are two options: 'Ephemeral' (unchecked) and 'Persistent' (checked). In the center, there are four input fields arranged in a grid-like layout. The first row contains 'VM Template' (labeled 'Required') with the value 'Windows10EVDr3500ver1' and a delete button ('x'). The second row contains 'Machine Size Type' (labeled 'Required') with the value 'Standard_E8as_v4' and a delete button ('x'). The third row contains 'Machine Storage Type' (labeled 'Required') with the value 'StandardSSD_LRS' and a delete button ('x'). The fourth row contains 'Number of Instances' with the value '12' in a dropdown menu. At the bottom right of the dialog are two buttons: 'Cancel' and 'Save', with 'Save' being highlighted.

4. Select the latest **VM Template**. Make the appropriate **Machine Size** and **Storage Type** selections based on your requirements.
5. Enter the **Number of Instances** equal to the total number of required Session Hosts. Typically this will be the same number as are currently in the Host Pool but it can be any number.
 - a. Note that the Session Hosts currently in the Host pool will ultimately be decommissioned after these new host come online. Plan for the **Number of Instances** entered to be sufficient to support the entire workload in this Host Pool.
6. Click **Save**, the session hosts will build based on the selected VM Template and starting coming online in as soon as 10-15 minutes (depending on the hypervisor).
7. When a new host comes online, the default setting is to stay in **Disallow New Sessions**. For each session host, the **Allow New Sessions** toggle can be used to manage which hosts can receive new user sessions. Once sufficient new hosts have been built and functionality has been confirmed, this setting can be managed on both the new and old hosts to route all new sessions to the new hosts. The old hosts, with **Allow New Sessions** set to **disabled**, can continue to run and host existing user sessions.

8. As users log off of the old host(s), and with no new user sessions joining the old host(s), the old host(s) where **Sessions = 0** can be deleted by clicking the **Actions** icon and selecting **delete**.

VDS Logical Hierarchy Overview

Overview

VDS organizes concepts into various layers of a logical hierarchy. This article helps to outline how they fit together.

VDS Organizational Scheme

The VDS management portal is found at <https://manage.vds.netapp.com>. This web interface is a single pane of glass for managing all VDS-related objects. Within the VDS web UI, the following hierarchy of components and logical containers exist.

VDS Deployment

The *Deployment* is a VDS concept that organized and contains *VDS Workspace(s)*. In certain deployment

architectures a deployment can contain multiple VDS Workspaces.



Running multiple VDS Workspaces within a single Deployment is called "Multi-Tenancy" and is only an option in RDS deployments, AVD deployments do not support this approach.

A deployment is defined by its Active Directory domain and there is a 1:1 relationship between the AD domain and a Deployment.

There are certain VM resources that are deployed to support a deployment that are shared across all VDS Workspaces in the deployment. E.g. every Deployment contains a VM named "CWMGR1" which is a server that run VDS applications, a SQL Express database and facilitates management of the VDS Workspace(s) (and the contained resources) within the Deployment.

VDS Workspace



There is a difference between a "**VDS Workspace**" and a "**AVD Workspace**".

A VDS Workspace is a logical container inside the deployment for the client (end user) resources. These resources include Virtual Machines (for session hosts, application servers, database servers, file servers etc.), virtual networking, storage and other hypervisor infrastructure.

The VDS Workspace also contains management functionality to manage Users, Security Groups, Workload Scheduling, Applications, Automation, VMs, and AVD configuration.

Typically a VDS Workspace is aligned with a single company, or (in enterprise deployments), a business unit.

VDS Sites

Within a deployment, multiple Sites can be created to represent different infrastructure providers, all managed within a single deployment.

This is helpful when a single company or business unit needs to host users and apps across multiple physical locations (e.g North America and EMEA), hypervisor subscriptions (to align costs to business units)and even hypervisors (E.g. users in Azure, Google Compute and on-premises HCI on vSphere).

AVD Workspaces



There is a difference between a "**VDS Workspace**" and a "**AVD Workspace**".

A AVD Workspace is a logical container that sits inside a VDS Workspace and VDS Site. It that can be used similarly to a VDS Site for segmenting management and operational policies in the same deployment.

AVD Host Pools

AVD Host Pools are logical container that sit inside a AVD Workspace and hold the Session Hosts and App Groups users to server the user sessions and control access to individual resources.

AVD App Groups

Each AVD Host Pool starts with a single "Desktop" App Group. Users and/or groups can be assigned to this (or other) App Group to allow access to the resources in the App Group to the assigned users.

Additional App Groups can be created within a host pool in VDS. All Additional App Groups are "RemoteApp"

App Groups and serve RemoteApp resources as opposed to a full windows desktop experience.

Applications

Application Entitlement

Overview

VDS has a robust application automation and entitlement functionality built-in. This functionality allows users to have access to different applications while connecting to the same session host(s). This is accomplished by some custom GPOs hiding shortcuts along with automation selectively placing shortcuts on the users' desktops.



This workflow only applies to RDS deployments. For AVD application entitlement documentation, please see [Application Entitlement Workflow for AVD](#)

Applications can be assigned to users directly or via Security groups managed in VDS.

At a high level, the application provisioning process follows these steps.

1. Add App(s) to App Catalog
2. Add App(s) to the workspace
3. Install the Application on all Session Hosts
4. Select the Shortcut path
5. Assign apps to users and/or groups



Steps 3 & 4 can be fully automated with Scripted Events as illustrated below

NetApp

NetApp Virtual Desktop Service

Application Management

Toby vanRoojen
Product Marketing Manager
June, 2020

Video Walkthrough

Add applications to the App Catalog

VDS Application Entitlement starts with the App Catalog, this is a listing of all the applications available for deployment to end user environments.

To add applications to the catalog, follow these steps

1. Log in to VDS at <https://manage.cloudworkspace.com> using your primary admin credentials.
2. In the upper right, click the arrow icon next to your User Name and select Settings.
3. Click the App Catalog tab.
4. Click the Add App option in the Application Catalog title bar.
5. To add a group of applications, choose the Import Apps option.
 - a. A dialog will appear that provides an Excel template to download that creates the correct format for the application list.
 - b. For this evaluation NetApp VDS has created a sample application list for import it can be found [here](#).
 - c. Click on the Upload area and choose the application template file, click the Import button.
6. To add individual applications, choose the Add App button and a dialog box will appear.
 - a. Enter the name of the application.
 - b. External ID can be used to enter an internal tracking identifier such as a product SKU or billing tracking code (optional).
 - c. Check the Subscription box if you want to report on the applications as a Subscription product (optional).
 - d. If the product does not install by version (for example Chrome) check the Version Not Required checkbox. This allows “continuous update” products to be installed without tracking their versions.
 - e. Conversely, if a product supports multiple named versions (ex: Quickbooks) you need to check this box so that you can install multiple versions and have VDS specific each available version in the list of applications that can be entitled for and end user.
 - f. Check “No User Desktop Icon” if you don’t want VDS to provision a desktop icon for this product. This is used for “backend” products like SQL Server since end users don’t have an application to access.
 - g. “App Must be Associated” enforces the need for an associated app to be installed. For example, a client server application may require SQL Server or mySQL to be installed as well.
 - h. Checking the License Required box indicates that VDS should request a license file to be uploaded for an installation of this application before it sets the application status to active. This step is performed on the Application detail page of VDS.
 - i. Visible to All – application entitlement can be limited to specific subpartners in a multi-channel hierarchy. For evaluation purposes, click the Check Box so that all users can see it in their available application list.

Add the application to the Workspace

To start the deployment process you’ll add the app to the workspace.

To do this, follow these steps

1. Click Workspaces
2. Scroll down to Apps
3. Click Add

4. Check box the application(s), enter required information, click Add Application, click Add Apps.

Manually install the application

Once the application has been added to the Workspace you'll need to get that application installed on all session hosts. This can be done manually and/or it can be automated.

To manually install applications on session hosts, follow these steps

1. Navigate to Service Board.
2. Click on the Service Board Task.
3. Click on the Server Name(s) to connect as a local admin.
4. Install the app(s), confirm the shortcut to this app is found in the Start Menu path.
 - a. For Server 2016 and Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Go back to the Service Board Task, click Browse and choose either the shortcut or a folder containing shortcuts.
6. Whichever you select is what will be displayed on the end user desktop when assigned the app.
7. Folders are great when an app is actually multiple applications. e.g "Microsoft Office" is easier to deploy as a folder with each app as a shortcut inside the folder.
8. Click Complete Installation.
9. If required, open the created Icon Add Service Board Task and confirm the icon has been added.

Assign applications to users

Application entitlement is handled by VDS and application can be assigned to users in three ways

Assign Applications to Users

1. Navigate to the User Detail page.
2. Navigate to the Applications section.
3. Check the box next to all applications required by this user.

Assign users to an application

1. Navigate to the Applications section on the Workspace Detail page.
2. Click on the name of the application.
3. Check the box next to the users the application.

Assign applications and users to user groups

1. Navigate to the Users and Groups Detail.
2. Add a new group or edit an existing group.
3. Assign user(s) and application(s) to the group.

Application Entitlement Workflow for AVD

Overview

In a Azure Virtual Desktop (AVD) environment, application access is managed by app group membership.



This workflow only applies to AVD deployments. For RDS application entitlement documentation, please see [Application Entitlement Workflow for RDS](#)



AVD is a well documented service and there are many [public resources for information](#). VDS does not supersede the standard way that AVD operates. Rather, this article is designed to illustrate how VDS approaches the standard concept found across all AVD deployments.



Reviewing the [VDS Logical Hierarchy Overview](#) article may be useful before or while reviewing this article.

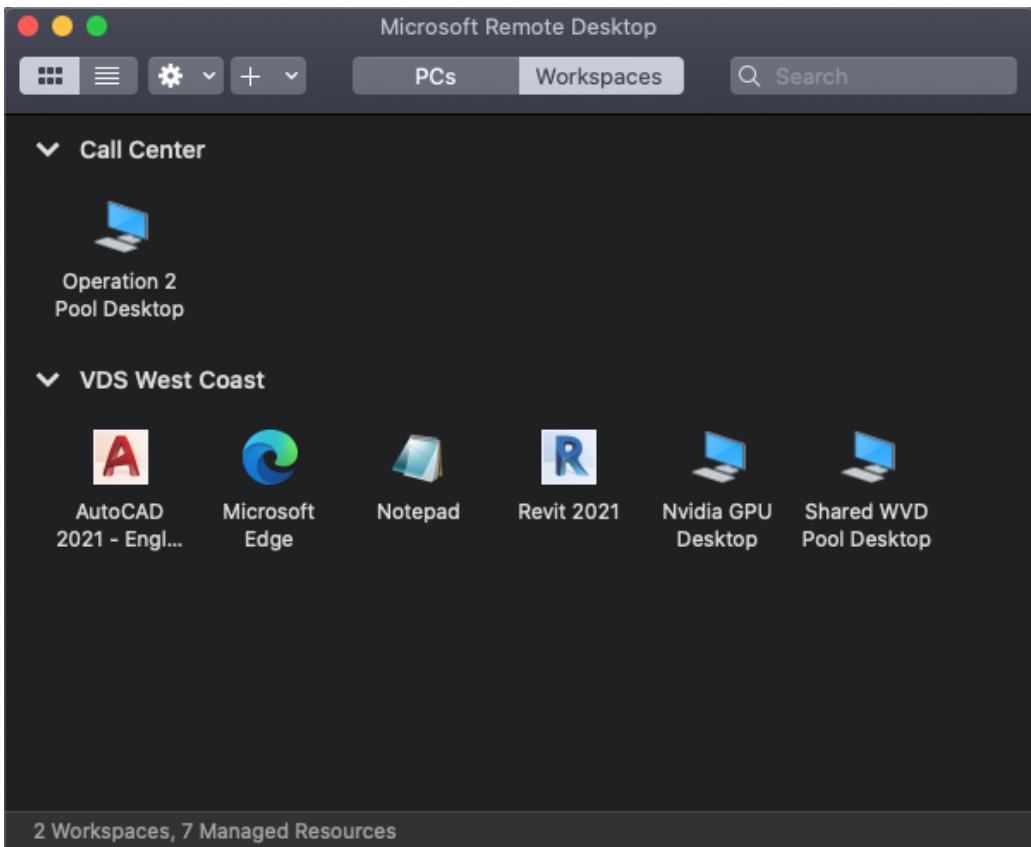
The End User View

In Azure Virtual Desktop, each end user is assigned access to RemoteApp(s) and/or Desktop(s) by their AVD administrator. This is accomplished via App Group assignment in VDS.

RemoteApp refers to an application that runs remotely on the session host but is presented on the local device without the desktop context. Commonly referred to as a "streaming app", these applications look like local applications on the local device but run in the security context, and on the storage and compute layer of the session host.

Desktop refers to the full Windows experience running on the session host and presented on the local device, typically in a full screen window. Commonly referred to as "remote desktop", this desktop itself will contain any applications installed on that session host which can be launched by the user from within the desktop session window.

At login, the end user is presented with the resources assigned to them by their administrator. Below is an example of the view an end user may see when logging in with their AVD client. This is a more complex example, often an end user will only have a single desktop or RemoteApp assigned to them. The end user can double click on any of these resources to launch that application/desktop.

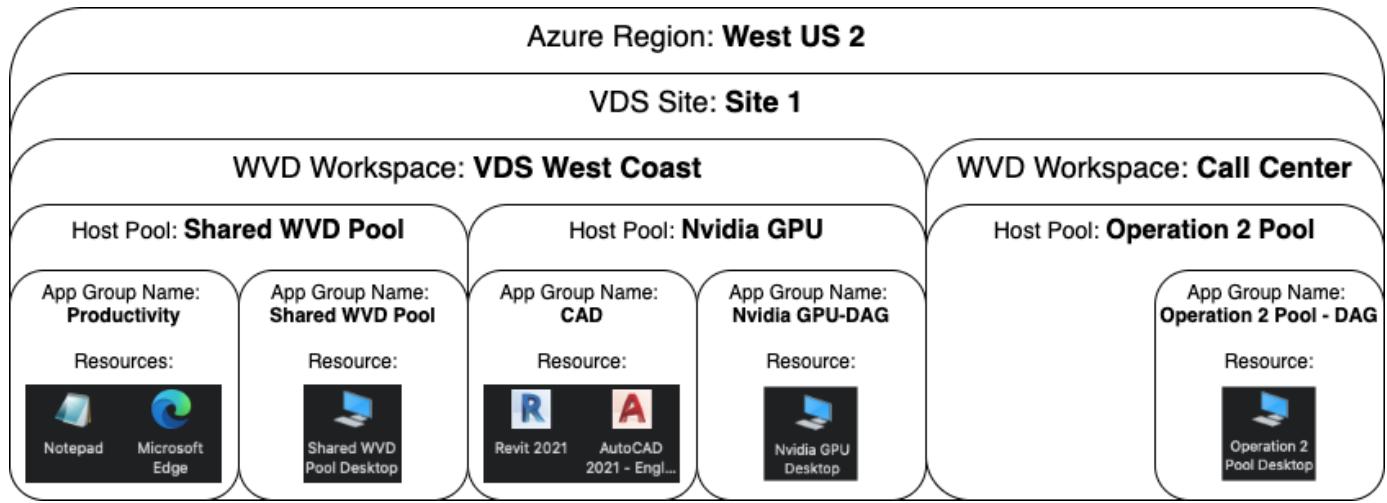


In this more complex example, this user has access to two different desktop sessions and 4 different streaming applications:

- **Available Desktops**
 - Nvidia GPU Desktop
 - Shared AVD Pool Desktop
 - Operation 2 Pool Desktop
- **Available RemoteApps**
 - AutoCAD 2021
 - Revit 2021
 - Microsoft Edge
 - Notepad

Behind the scenes these applications and desktops are hosted across a variety of session hosts, AVD workspaces and could even be hosted in different Azure regions.

Here is a diagram illustrating where each of these resources are hosted and how they got assigned to this end user.



As shown above, the various resources available to this end user are hosted in different session hosts, in different host pools, and potentially managed by different IT organizations in different AVD Workspaces. While not showing in this example, these resources could also be hosted in different Azure regions and/or subscriptions using the VDS Sites feature.

Providing Desktop Access

By default every host pool starts with a single app group, used to assign access to the Windows desktop experience. All applications installed on these session hosts will be accessible to the end users assigned to this app group.

To enable the Desktop resource for users in VDS:

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the App group for the "Desktop" resource.

[Management.Applications.AVD application entitlement workflow 349fe] |

Management.Applications.AVD_application_entitlement_workflow-349fe.png

2. Once inside the App Group, click Edit

[Management.Applications.AVD application entitlement workflow 3bcfc] |

Management.Applications.AVD_application_entitlement_workflow-3bcfc.png

3. From the edit dialog, you can add or remove users to this App Group by User and/or by Groups.

[Management.Applications.AVD application entitlement workflow 07ff0] |

Providing RemoteApp Access

In order to provision access to RemoteApps, a new app group needs to be created within the host pool. Once created, the appropriate apps need to be assigned to this app group.



Any applications on these sessions hosts will already be available to any users assigned to this host pool's "Desktop" AppGroup. It is not necessary to also provision access via a RemoteApp app group simply to provide access to apps. A RemoteApp app group is only necessary to enable access to apps that run as-if on the local device as a streaming app.

Create a New App Group

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the *+ Add App Group* button

[Management.Applications.AVD application entitlement workflow d33da] |

Management.Applications.AVD_application_entitlement_workflow-d33da.png

2. Enter the Name, Workspace and Friendly Name for this app group. Select the users and/or groups that should be assigned and click Save

[Management.Applications.AVD application entitlement workflow 242eb] |

Add Applications to the App Group

1. Navigate to the Workspaces > AVD > Host Pool > App Groups page and click on the App group for the "RemoteApp" resource.

[Management.Applications.AVD application entitlement workflow 3dcde] |

Management.Applications.AVD_application_entitlement_workflow-3dcde.png

2. Once inside the App Group, click Edit

[Management.Applications.AVD application entitlement workflow 27a41] |

Management.Applications.AVD_application_entitlement_workflow-27a41.png

3. Scroll down to the "Remote Apps" section. This section may take a moment to populate as VDS is directly querying the session hosts to show available apps for streaming.

[Management.Applications.AVD application entitlement workflow 1e9f2] |

4. Search and select any apps that the users in this app groups should have access to as a RemoteApp resource.

Scripted Events

Scripted Events

Overview

Scripted Events provides the advanced administrator with a mechanism to create custom automation for system maintenance, user alerts, group policy management, or other events. Scripts can be designated to run as an executable process with arguments, or can be used as arguments for a different executable program. This functionality allows for scripts to be combined and nested to support complex customization and integration needs.

A detailed example of scripted events in action is found in the [Application Entitlement Guide](#).

Additionally, Scripted Events allows for the creation of automation that does not require a script to process, rather the automation flow is launched by a system trigger and runs an existing program or system utility with optional arguments.

Scripted Events contains both a **repository** of scripts and **activities**. Scripts contain the instructions on **what** to do while activities link the scripts with the appropriate trigger and target (**when and where**) for the script.

Repository

The Repository Tab shows a list of all scripts available to be deployed from within your VDS account. This is a custom repository that is shared by all administrators in your VDS instance. Access to Scripted Events can be managed on the *VDS > Admins > Permissions page*.

The screenshot shows the NetApp Virtual Desktop Service interface. On the left, there's a sidebar with links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is highlighted), and Admins. The main area has a header with 'Home > Scripted Events' and a search bar. Below that is a 'Scripted Events' section with tabs for 'Repository' (which is selected and highlighted with a green box) and 'Activities'. There's a 'Filter By' section with a keyword search input and checkboxes for 'Customer' and 'Global'. At the bottom, there's a table with columns: Name, Script, Type, Created on, and Actions. Two rows are listed: 'Install Adobe Reader' (Script: InstallAdobeReader.ps1, Type: Customer, Created on: Dec 4, 2020, 12:39 PM) and 'Install Microsoft Office 365' (Script: InstallMicrosoftOffice365.ps1, Type: Customer, Created on: Dec 8, 2020, 9:57 AM). A 'Refresh' button and a '+ Add Script' button are also visible.

Name	Script	Type	Created on	Actions
Install Adobe Reader	InstallAdobeReader.ps1	Customer	Dec 4, 2020, 12:39 PM	⋮
Install Microsoft Office 365	InstallMicrosoftOffice365.ps1	Customer	Dec 8, 2020, 9:57 AM	⋮

Customer Filter

Each VDS administrator organization has a private library of scripts created and/or customized by their organization. These scripts are defined as Script Type "Customer." Customer scripts can be deleted and edited by any VDS administrator with appropriate admin permissions to the Scripted Events section.

Global Filter

NetApp also publishes and maintains a library of "Global" scripts that is the same across all VDS administrator organizations. These scripts are defined as Script type "Global." Global scripts can not be edited or deleted by any VDS administrator. Rather, Global scripts can be "Cloned" and the resulting script is a "Customer" script that can be edited and used.

Download Script

The ability to download the script file associated with a Scripted Event allows the VDS Administrator to review and edit the underlying script file prior to deployment. Running a script that you don't fully understand is never advisable.

The screenshot shows the 'Scripted Events' page. On the left is a sidebar with links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected), Admins, and Reports. The main area has tabs for 'Repository' (selected) and 'Activities'. A search bar and a 'Toby' user icon are at the top right. Below is a table with columns: Name, Script, Type, Created on, and Actions. Three scripts are listed: 'Install Adobe Reader', 'Install AMD Radeon Instinct Drivers', and 'Install Ezeep Print App'. The third script's row has a context menu with 'Download' and 'Clone' options, both of which are highlighted with a green border.

Name	Script	Type	Created on	Actions
Install Adobe Reader	InstallAdobeReader.ps1	Global	Jan 12, 2021, 12:42 PM	⋮
Install AMD Radeon Instinct Drivers	InstallAMDRadeonInstinctDrivers.ps1	Global	Jan 12, 2021, 12:25 PM	⋮
Install Ezeep Print App	InstallEzeepPrintApp.ps1	Global	Jan 12, 2021, 12:41 PM	⋮ Download Clone

Add Script

Clicking on the **+ Add Script** button opens a new page for creating a script and saving it to the repository.

The screenshot shows the 'Add Script' form. It includes fields for 'Name' (with 'Required' validation), 'Include Script File' (radio buttons for 'Yes' and 'No', with 'Yes' selected), 'Execute With' (set to 'rShell\vl1.0\powershell.exe'), 'Arguments' ('-file %scriptname%'), and 'Documentation URL' (a link to a Microsoft Edge Chromium documentation page). At the bottom are 'Cancel' and 'Add Script' buttons, with 'Add Script' being the active one.

The following fields need to be completed to create a new script:

- **Name**
- **Include Script File**
 - Yes - Allows for a script file (e.g. a .ps1 file) to be uploaded and run by the "Execute With" executable.
 - No - Removes the "Script File" field (below) and simply runs the "Execute With" and "Arguments" command

- **Script File**

- If *Include Script File* = Yes this field is visible and allows for the upload of a script file.

- **Execute With**

- Defines the path of the executable that is used to run the script file or the command that is run.
- For example, to run with PowerShell the "Execute With" value would be
C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

- **Arguments**

- Defines any additional arguments that are run against the "Executes With" command.
- VDS offers some context aware variables that can be used including:
 - %companycode% - Company code at runtime
 - %servername% - VM name at runtime
 - %samaccountname% - <username>.<companycode>
 - %applicationname% - Requested application name at runtime
 - %scriptname% - Script name at runtime
 - %username% - username@loginidentifier at runtime

- **Documentation URL**

- This field allows the writer of the script to link it to documentation found outside of VDS such as a Knowledge Base system used by the VDS admins' organization.

Edit Script

Clicking the name of a script in the repository opens a new page with details about the script and an action button to **edit**.

When editing a script the same fields are editable as documented above in the [Add Script](#) section.

On this script detail page, you can also **delete** the script and **download** any uploaded script file.

The screenshot shows the NetApp Virtual Desktop Service web interface. On the left is a dark sidebar with various navigation options like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events, Admins, Reports, Applications, Cost Estimator, and SaaS Backup. The 'Scripted Events' option is highlighted. The main content area has a header 'Home > Scripted Events > Install Microsoft Office 365'. Below the header, the title 'Install Microsoft Off...' is displayed, followed by a 'Script' tag and an 'Overview' tab (which is selected). The 'Script Details' section contains the following information:

Name	Type	
Install Microsoft Office 365	Customer Script	
Script	Execute With	Arguments
InstallMicrosoftOffice365.ps1	C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe	-file %scriptname%
Created By	Created On	
toby.vanrooijen@vdsdocsdemo	Dec 8, 2020, 9:57 AM	
Updated By	Updated On	
None	None	
Documentation URL	https://docs.netapp.com/us-en/virtual-desktop-service/scriptlibrary/MicrosoftOffice365.html	

At the top right of the main content area, there are buttons for Refresh, Download (highlighted with a green border), Edit, and a more options menu. A search bar and a user profile for 'Toby' are also visible at the very top of the page.

Activities

Activities link a script from the repository to a Deployment, a subset of VMs and a trigger event.

The screenshot shows the 'Scripted Events' section of the NetApp Virtual Desktop Service. On the left is a sidebar with links like Home, Organizations, Deployments, Workspaces, App Services, Service Board, Scripted Events (which is selected and highlighted in blue), and Admins. The main area has a header 'Scripted Events' with tabs for 'Repository' and 'Activities'. A green box highlights the 'Activities' tab. Below is a search bar and a 'Filter By' dropdown. A table lists two activities: 'InstallAdobeReader' and 'UninstallAdobeReader'. Each row includes columns for Name, Script, Deployment, Event, Clients, App Services, Enabled (with a checkmark), and Actions (with a three-dot menu icon). Buttons for 'Refresh' and '+ Add Activity' are at the bottom right.

Add Activity

Clicking on the **+ Add Activity** button opens a new page for creating an Activity.

The screenshot shows the 'Add Activity' page. The left sidebar is identical to the previous one. The main area has a header 'Add Activity'. It contains several sections: 'Activity Settings' (Name: 'Install Chrome', Description: 'Install Chrome'), 'Deployment' (Deployment: 'VDSGCPDemo (kxk)', Script: 'InstallGoogleChrome', Arguments: 'Enter arguments...'), an 'Enabled' checkbox checked, 'Event Settings' (Event Type: 'Application Install'), 'Target Settings' (Application: 'Google Chrome', Shortcut Path: '\\shortcuts\\Google Chrome.lnk'), and a 'Required' status indicator. At the bottom are 'Cancel' and 'Add Activity' buttons.

The following fields need to be completed to create a new activity:

- **Name**
- **Description (Optional)**
- **Deployment**
- **Script**
- **Arguments**
- **Enabled** checkbox
- **Event Settings**

Activity Triggers

• Application Install

- This is triggered when the VDS Admin clicks "+ Add..." from the *Workspace > Applications* page.
- This selection allows you to select an application from the Application Library and to pre-define the shortcut of the application.
- Detailed instructions for this trigger are highlighted in the [Install Adobe Reader DC script documentation](#).

• Application Uninstall

- This is triggered when the VDS Admin clicks **Actions > Uninstall** from the *Workspace > Applications* page.
- This selection allows you to select an application from the Application Library and to pre-define the shortcut of the application.
- Detailed instructions for this trigger are highlighted in the [Uninstall Adobe Reader DC script documentation](#).

• Clone Server

- This is triggered when the Clone function is performed against an existing VM

• Create Cache

- This is triggered anytime a new VM is built by VDS for a provisioning collection cache

• Create Client

- This is triggered anytime a new Client organization is added to VDS

• Create Server

- This is triggered anytime a new VM is built by VDS

- **Create User**

- This is triggered anytime a new user is added via VDS

- **Delete User**

- This is triggered anytime a new user is deleted via VDS

- **Manual**

- This is triggered by a VDS admin manually from within the **Scripted Events > Activity** page

- **Manual Application Update**

- **Scheduled**

- This is triggered when the defined date/time is reached

- **Start Server**

- This is triggered on a VM each time it boots up

Clicking on the *Name* opens a dialog box where the activity can be edited.

Command Center

Command Center Command: Overview

Overview

The Command Center is an executable that runs on the CWMGR1 Platform Server in the Deployment. It is accessed by connecting to the CWMGR1 VM and executing it locally on that VM.

This application was designed for troubleshooting, diagnostic and advanced management functions. This application is primarily used by NetApp's internal development and support teams however some functions are occasionally used by customer admins. This documentation is provided to support the use of selection functions. Use of these commands should be done with care and in collaboration with the NetApp support team.

Running Command Center

To run the Command Center application:

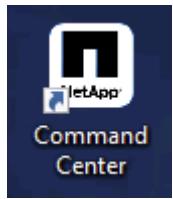
1. Connect to the server from the *VDS > Deployment > Platform Servers* page click the *Actions* icon and select "Connect"

Name	CPU	RAM (GB)	Online	Actions
CWMGR1	2	8	Online	Request Backup Connect

2. When prompted for credentials enter domain admin credentials
 - a. The user will need to be a member of the "CW-Infrastructure" security group. For consistency sake we recommend adding this membership by making the user a member fo the "Level 3 Technicians" group in AD > Cloud Workspace > Cloud Workspace Tech Users > Groups

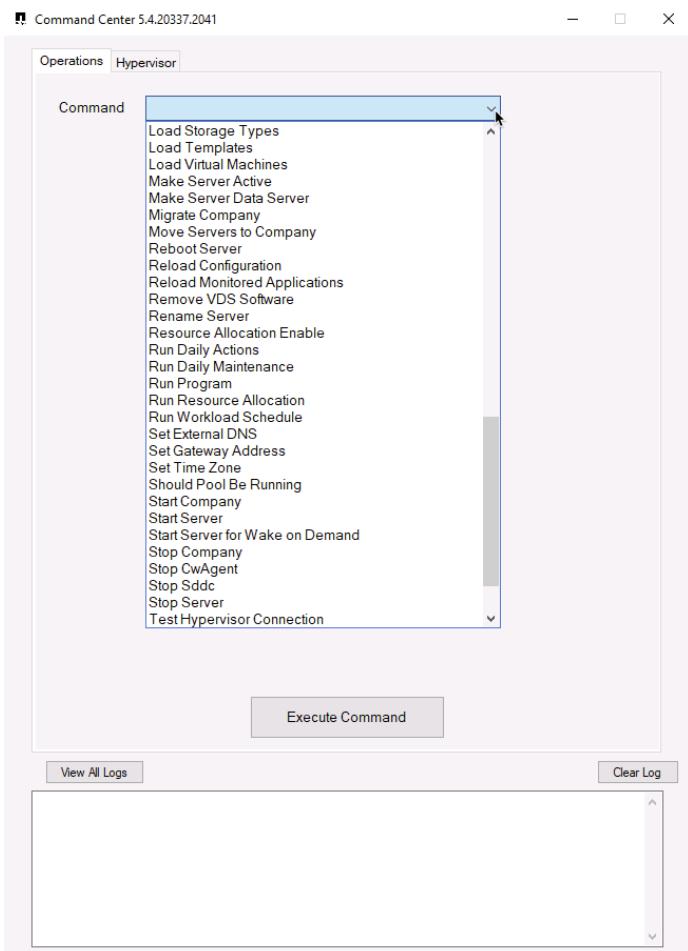
Name	Type	Description
CW-CWMGRAccess	Security Group...	CW-CWMGRAccess - en...
Level3 Technicians	Security Group...	Level 3 technicians - en...

3. Locate the desktop icon for *Command Center* and run it



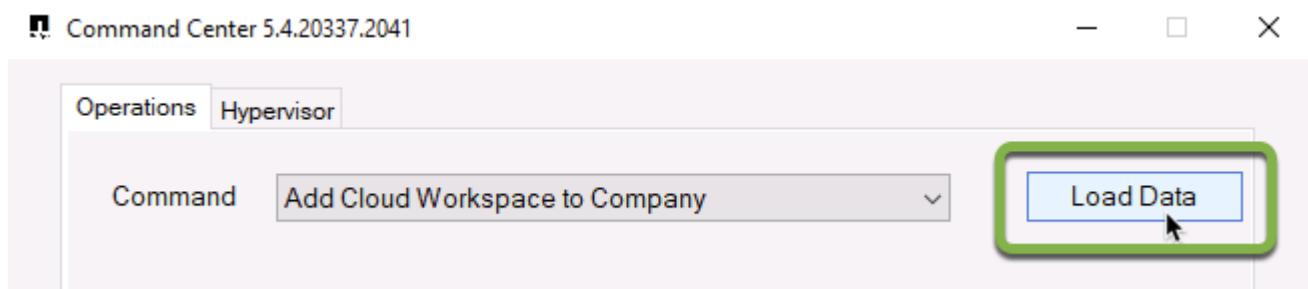
- a. To enable the advanced tab, launch the application with the "-showadvancedtab" switch.

Operations Tab



From the **Command** menu you can select from a list of actions (listed below).

Once a command is selected, data can be populated with deployment data from the **Load Data** button. The Load Data button is also used to query the hypervisor for data once earlier selections are made (e.g. Loading a list of available backup dates after selecting a specific VM from a dropdown)



After making selections on a command, clicking **Execute Command** will run the selected process.

To review logs, click the **View All Logs** button. The raw text file will open, with newest entries at the bottom.

Command List

- [Copy Template to Gallery](#)

Operations

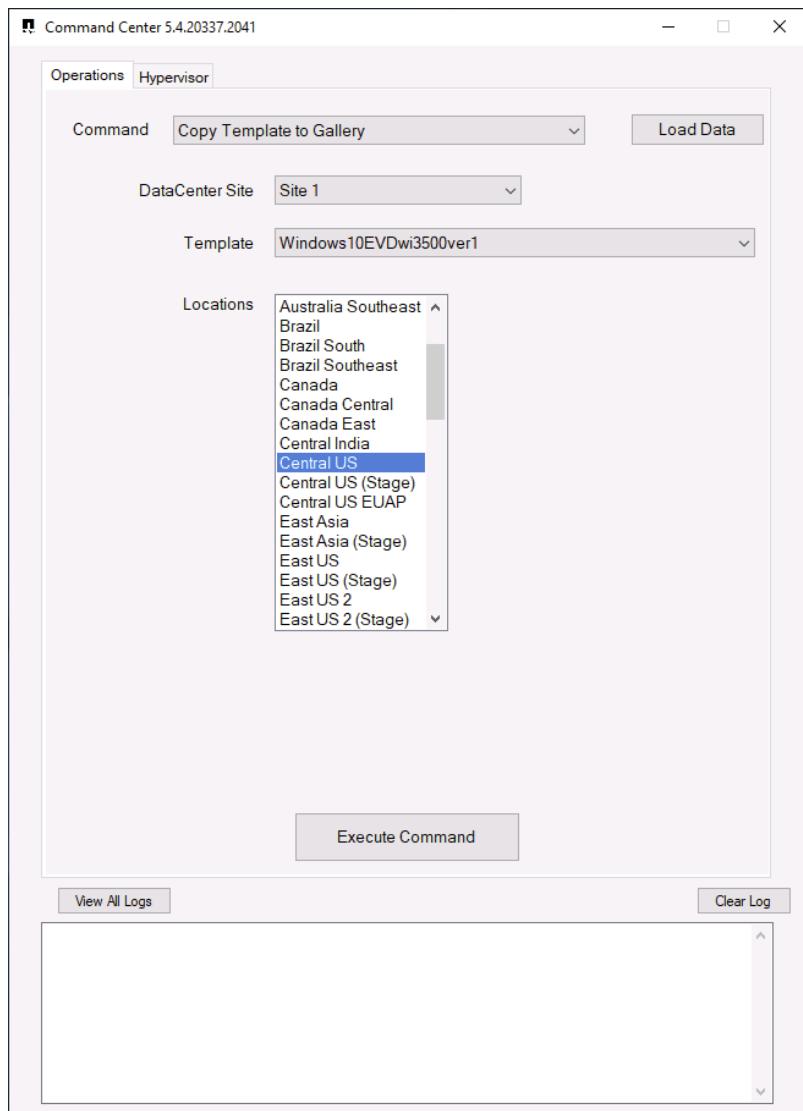
Command Center Command: Copy Template to Gallery

Command Center Warning



The Command Center is an application that runs on the CWMGR1 Platform Server in the Deployment. This application was designed for troubleshooting, diagnostic and advanced management functions. This application is primarily used by NetApp's internal development and support teams however some functions are occasionally used by customer admins. This documentation is provided to support the use of selection functions. Use of these commands should be done with care and in collaboration with the NetApp support team. More information can be found in the [Command Center Overview](#) article.

Copy Template to Gallery Overview



When a VDI Provisioning Collection is finalized the image is stored in Azure as an Image and can be deployed within the same VDS Site. In order to make the image available for deployment in another Azure region within the same Subscription the "Copy Template to Gallery" function is used. This action will copy the VM image to the Shared gallery and replicate it to all the selected regions.

VM Template Availability in VDS Dropdown

Once the replication has completed, the image will show in VDS in the dropdown for selecting VM Templates when deploying new VMs. The shared image will be available for deployment into any region that is selected when copying.

The screenshot shows the Azure portal interface for a shared image gallery named 'YBY_Site1'. The main pane displays the details for the image 'Windows10WVDNo3503ver1'. The 'Essentials' section includes fields like Resource group (yby), Status (Succeeded), Location (West US 2), Subscription (Azure subscription 1), and SKU (Windows10WVDNo3503ver1). The 'Image versions' section shows a single version entry: Name (1.0.0), Provisioning state (Creating), Source image (Windows10WVDNo3503ver1), Target regions (2), Storage account type (Standard HDD), and Replication status (InProgress). The left sidebar lists other options like Overview, Activity log, Tags, and Configuration.

VM Images stored in the Shared Gallery are appended with their version in the form of "-x.x.x" where the version matches the image version within the Azure Portal.

The screenshot shows a dropdown menu titled 'VM Template' with the heading 'Required'. It contains two items: '3500' and 'Windows10EVDwi3500ver1-1.0.0'. The second item is highlighted with a yellow background, indicating it is the selected or replicated version.



The replication of the image can take a while (depending on the size of the image) and the status can be seen by clicking on the version (e.g. 1.0.0) in the "Name" column as highlighted in the screenshot above.

Regional Availability

Deployments can only be performed into the regions where the image has been replicated. This can be checked in the Azure portal by clicking on the 1.x.x and then on *Update Replication* as shown here:

Microsoft Azure Search resources, services, and docs (G+ /) admin@VDSazuredemo... VDS SALES DEMO

Home > Shared image galleries > YBY_Site1 > Windows10EVD3497ver1 (YBY_Site1/Windows10EVD3497ver1) > 1.0.0 (YBY_Site1/Windows10EVD3497ver1/1.0.0)

1.0.0 (YBY_Site1/Windows10EVD3497ver1/1.0.0) | Update replication

Image version

Search (Cmd+/) Save Discard Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Update replication Configuration Properties Locks Automation Tasks (preview) Export template Support + troubleshooting New support request

Target regions Target region repli... Storage account type Replication status

Target regions	Target region repli...	Storage account type	Replication status
(US) Central US	1	Standard HDD	Completed
(US) West Cent...	1	Standard HDD	Completed
(US) West US 2	1	Standard HDD	Completed
		Standard HDD	-

Resource Optimization

Workload scheduling

Workload Scheduling is a feature that can schedule the time window in which the environment is active.

Workload scheduling can be set to "Always On", "Always Off" or "Scheduled". When set to "Scheduled" the on and off times can be set as granularly as a different time window for each day of the week.

5.4 Preview

Edit Workload Schedule

Status

Scheduled

Scheduling Options

- Run at assigned time interval everyday
- Run at assigned time interval on specified days
- Run at variable time interval and days

Days

Sun Mon Tue Wed Thu Fri Sat

Current Schedule

4 Day(s) Scheduled.

Cancel Update Schedule

When scheduled to be off, either via "Always Off" or "Scheduled", all tenant virtual machines will shut down. Platform servers (such as CWMGR1) will remain active to facilitate functionality such as wake on demand.

Workload Schedule works in conjunction with other resource optimization features including Live Scaling and Wake on Demand.

Wake on demand

Wake on Demand (WoD) is patent-pending technology that can wake the appropriate VM resources for an end user in order to facilitate unattended access 24/7, even when resources are scheduled to be inactive.

WoD for Remote Desktop Services

In RDS, the VDS Windows Client has built-in Wake on Demand integration and can wake the appropriate resources without any additional end-user actions. They simply need to initiate their normal login and the client will notify them of a short delay which the VM(s) are activated. This client (and thus this automate wake on demand functionality) is only available when connecting from a Windows device to an RDS environment.

Similar Functionality is built into the VDS Web client for RDS deployments. The VDS Web Client is found at: <https://login.cloudworkspace.com>

Wake on Demand functionality is not built into the Microsoft RD client (for Windows or any other platform) nor

any other 3rd party RD clients.

Wake on demand for Azure Virtual Desktop

In AVD, the only clients that can be used to connect are Microsoft provided and thus do not contain the Wake on Demand functionality.

VDS does include a self-service Wake on Demand function for AVD via the VDS Web Client. The web client can be used to wake the appropriate resources, then the connection can be initiated via the standard AVD client.

To wake VM resources in AVD:

1. Connect to the VDS Web Client at <https://login.cloudworkspace.com>
2. Login with the user AVD credentials
 - A warning message will prompt "*You have Microsoft's AVD services available. Click HERE to view the status and start offline Host Pools.*"
3. After clicking "*HERE*" you'll see a list of available Host Pools along with a link to "Click to Start" link under the status column

Host Pool	Status
Test JG 2 tenant	● Online Click to Start

[Return to Login](#)

4. *Click to Start* the link and wait 1-5 minutes for the status to change to "Online" and show a green status icon
5. Connect to AVD using your normal process

Live Scaling

Live Scaling works in conjunction with Workload Scheduling by managing the number of online session hosts during the scheduled active time as configured in Workload Scheduling. When scheduled to be offline, Live Scaling won't control session host availability. Live scaling only impacts Shared Users and Shared Servers in RDS and AVD environments, VDI Users and VDI VMs are excluded from these calculations. All other VM types are unaffected.



The AVD *load balancer type* setting interacts with this configuration, so care should be taken in choosing that setting as well. Cost savings are maximized with a depth-first type while end user performance is maximized with a breadth-first type.

Enabling Live Scaling with no options checked, the automation engine will automatically select values for the Number of Extra Powered on Servers, Shared Users Per Server, and Max Shared Users Per Server.

- The *Number of Extra Powered on Servers* defaults to 0, meaning 1 server will run 24/7.
- The *Shared Users Per Server* defaults to the number users in the company divided by the number of servers.
- The *Max Shared Users Per Server* defaults to infinite.

Live Scaling turns the servers on as users log on and turns them off as users log off.

Powering an additional server is automatically triggered once the total active users reaches the number of Shared Users per Server multiplied by the total number of Powered On Servers.

e.g. With 5 Shared Users per Server set (this is the default # we'll use for all examples in this article) and 2 servers running, a 3rd server won't be powered up until server 1 & 2 both have 5 or more active users. Until that 3rd server is available, new connections will be load balanced all available servers. In RDS and AVD Breadth mode, Load balancing sends users to the server with the fewest active users (like water flowing to the lowest point). In AVD Depth mode, Load balancing sends users to servers in a sequential order, incrementing when the Max Shared Users number is reached.

Live Scaling will also turn off servers to save costs. When a server has 0 active users, and another server has available capacity below *Shared Users per Server* the empty server will be powered down.

Powering on the next server can take a few minutes. In certain situations the speed of logins can outpace the availability of new servers. For example, if 15 people login in 5 minutes they'll all land on the first server (or be denied a session) while a 2nd and 3rd power up. There are two strategies that can be used to mitigate overloading a single server in this scenario:

1. Enable *Number of Extra Powered on Servers* so that the additional server(s) will be on and available to accept connections and allow time for the platform to spin up additional servers.
 - a. When activated, the number is added to the calculated need. For example, if set to 1 extra server (and with 6 users connected) two servers would be active because of the users count, plus a 3rd due to the *Extra Powered on Servers* setting.
2. Enable *Max Shared Users Per Server* to place a hard limit on the number of users allowed per server. New connections that would exceed this limit will be refused, the end user will get an error message and need to try again in a couple minutes once the additional server is available. If set, this number also defines the depth of AVD Shared servers.
 - a. Assuming the delta between *Shared Users Per Server* and *Max Shared Users Per Server* is appropriate, the new servers should become available before the max is reached in all but the most extreme situations (unusually large login storms).

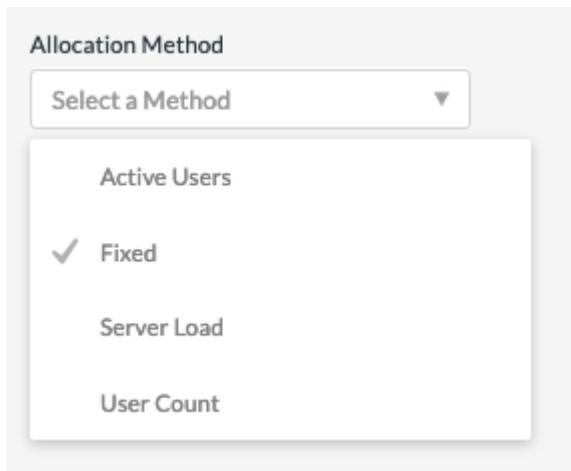
VM resource scaling

VM Resource scaling is an optional feature that can change the size and quantity of session host VMs in an environment.

When activated, VDS will calculate the appropriate size and quantity of session host VMs based on your selected criteria. These options include: Active Users, Named Users, Server Load, and Fixed.



The size of the VMs is contained within the family of VMs selected in the UI which can be changed by dropdown.
(e.g. Standard Dv3 Family in Azure)



Scaling based on users



The function below behaves the same for either "Active Users" or "User Count". User Count is a simply count of all users activated with a VDS desktop. Active Users is a calculated variable based on the previous 2 weeks of user session data.

When calculating based on users, the size (and quantity) of the session host VMs is calculated based on the defined RAM and CPU requirements. The administrator can define the GB of RAM, and number of vCPU cores per user along with additional non-variable resources.

In the screenshot below, each user is allocated 2GB RAM and 1/2 of a vCPU core. Additionally, the server starts with 2 vCPU cores and 8GB RAM.

The screenshot shows two configuration sections. The top section, titled 'Per User Settings', contains fields for 'RAM per User (GB)' set to 2 and 'CPU Per User' set to .5. The bottom section, titled 'Additional Resources per Server', contains fields for 'Additional RAM (GB)' set to 8 and 'Additional CPUs' set to 2.

Additionally, the administrator can define the maximum size a VM can reach. When reached, environments will scale horizontally by adding additional VM session hosts.

In the screenshot below, each VM is limited to 32GB Ram and 8vCPU cores.

The screenshot shows the 'Server Capacity' settings. It includes a slider for 'Max RAM (GB)' ranging from 1 to 240, with a current value of 32. It also includes a slider for 'Max CPU' ranging from 1 to 64, with a current value of 8.

With all of these variables defined, VDS can calculate the appropriate size and quantity of session host VMs, greatly simplifying the process of maintaining appropriate resource allotment, even as users are added and removed.

Scaling based on server load

When calculating based on server load, the size (and quantity) of session host VMs is calculated based on the average CPU/RAM utilization rates as observed by VDS over the previous 2-week period.

When the maximum threshold is exceeded, VDS will increase the size or increment the quantity to bring average usage back within range.

Like user based scaling, the VM Family and the maximum VM size can be defined.

The screenshot shows the 'Manage Resource Pool' interface. It includes sections for 'Basic Resource Info', 'Server Load Settings', and 'Server Capacity'. In 'Basic Resource Info', there are fields for 'Name' (Primary Host Pool), 'Status' (Enabled), and 'Allocation Method' (Server Load). Under 'Server Load Settings', there are 'Peak Hourly Resource Usage' tables for RAM and CPU, both showing 0% usage. There are also 'Increase Resource Threshold' and 'Decrease Resource Threshold' sections for RAM and CPU, each with a slider set at 70%. In 'Server Capacity', sliders are shown for 'Max RAM (GB)' (set to 240) and 'Max CPU' (set to 64), with current values of 32 and 8 respectively. At the bottom are 'Cancel' and 'Apply to Servers' buttons.

Other active resources

Workload Scheduling does not control the platform servers such as CWMGR1 as they are needed to trigger the Wake on Demand functionality and facilitate other platform tasks and should run 24/7 for normal environmental operation.

Additional saving can be achieved by deactivating the entire environment but is only recommended for non-production environments. This is a manual action that can be performed in the Deployments section of VDS. Returning the environment to a normal status also requires a manual step on the same page.

Deployment URL	VDS	Azure	VM Progress (Provisioning)
bw54deploy.onmicrosoft.com	skk	5.4	Azure 1 ● Offline ● Available Delete
cjdevmherr2.onmicrosoft.com	pht	5.4	Azure 1 ● Online ● Available Stop Gear

							Delete
bw54deploy.onmicrosoft.com	skk	5.4	Azure	1	● Offline	● Available	Start
cjdevmherr2.onmicrosoft.com	pht	5.4	Azure	1	● Online	● Available	Start

User Administration

Managing User Accounts

Create New User(s)

Admins can add Users by clicking Workspaces > Users and Groups > Add/import

Users can be added individually or with a bulk import.



Including accurate email and mobile phone # at this stage greatly improves the process of enabling MFA later.

Once you have created Users, you can click on their name to see details like when they were created, their connection status (whether they're currently logged in or not) and what their specific settings are.

Activating the Virtual Desktop for existing AD users

If users are already present in AD, you can simple activate the users' Virtual Desktop by clicking on the gear next to their name and then enabling their desktop.



For Azure AD Domain Service only: In order for logins to work, the password hash for Azure AD users must be synced to support NTLM and Kerberos authentication. The easiest way to accomplish this task is to change the user password in Office.com or the Azure portal, which will force the password hash sync to occur. The sync cycle for Domain Service servers can take up to 20 minutes so changes to passwords in Azure AD typically take 20 minutes to be reflected in AADDS and thus in the VDS environment.

Delete user account(s)

Edit user info

On the user detail page changes can be made the the user details such as username and contact details. The email and phone values are used for the Self Service Password Reset (SSPR) process.

User Details

Username	TFranklin
Phone	Email
	
Login Identifier	Partner VDS Sales

Edit user security settings

- VDI User Enabled – an RDS Setting that, when enabled, builds a dedicated VM session host and assigned this user as the only user that connect to it. As part of activating this checkbox the CWMS administrator is prompted to select the VM Image, Size and Storage Type.
 - AVD VDI users should be managed on the AVD page as a VDI host pool.
- Account Expiration Enabled – allows the CWMS administrator to set an expiration date on the end user account.
- Force Password Reset at Next Login – Prompts the end user to change their password at next login.
- Multi-Factor Auth Enabled – Enables MFA for the end user and prompts them to setup MFA at next login.
- Mobile Drive Enabled – A legacy feature not used in current deployments of RDS or AVD.
- Local Drive Access Enabled – Allows the end user to access their local device storage from the cloud environment including Copy/Paste, USB Mass storage and system drives.
- Wake on Demand Enabled – For RDS users connecting via the CW Client for Windows, enabling this will give the end user permission to take their environment when connecting outside of normal working hours as defined by Workload Schedule.

Locked Account

By default, five failed login attempts will lock the user account. The user account will unlock after 30 minutes unless *Enable Password Complexity* is enabled. With password complexity enabled, the account will not automatically be unlocked. In either case, the VDS admin can manually unlock the user account from the Users/Groups page in VDS.

Reset user password

Resets the user password.

Note: When resetting Azure AD user passwords (or unlocking an account) there can be a delay of up to 20 minutes as the reset propagates through Azure AD.

Admin Access

Enabling this give the end user limited access to the management portal for their tenant. Common uses include providing an on-site employee access to reset peers' passwords, assign application or allow manual server

wakeup access. Permissions controlling what areas of the console can be seen is set here as well.

Logoff user(s)

Logged on users can be logged off by the VDS admin from the Users/Groups page in VDS.

Applications

Displays the application deployed in this workspace. The check box provisions the apps to this specific user. Complete Application Management documentation can be found here. Access to applications can also be granted from the App interface or to Security Groups.

View/kill user processes

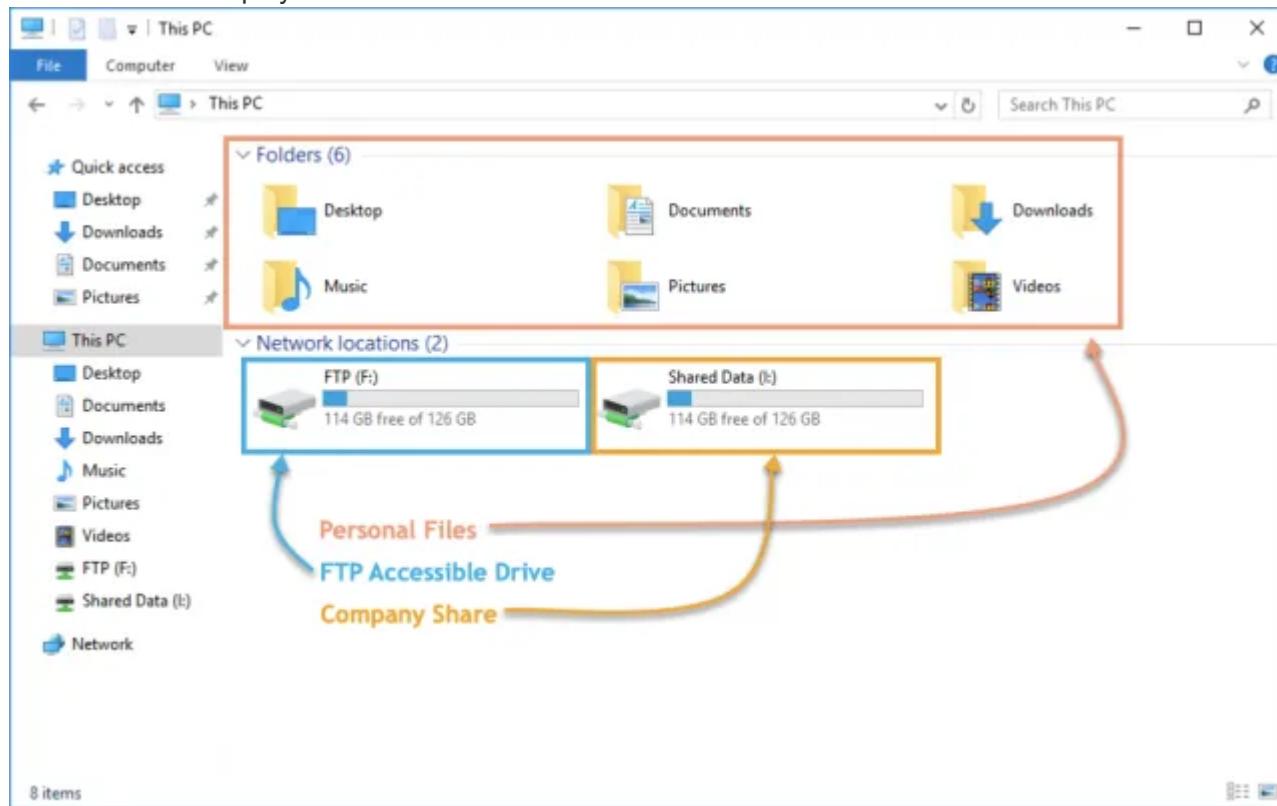
Displays the processes currently running in that user's session. Processes can be ended from this interface as well.

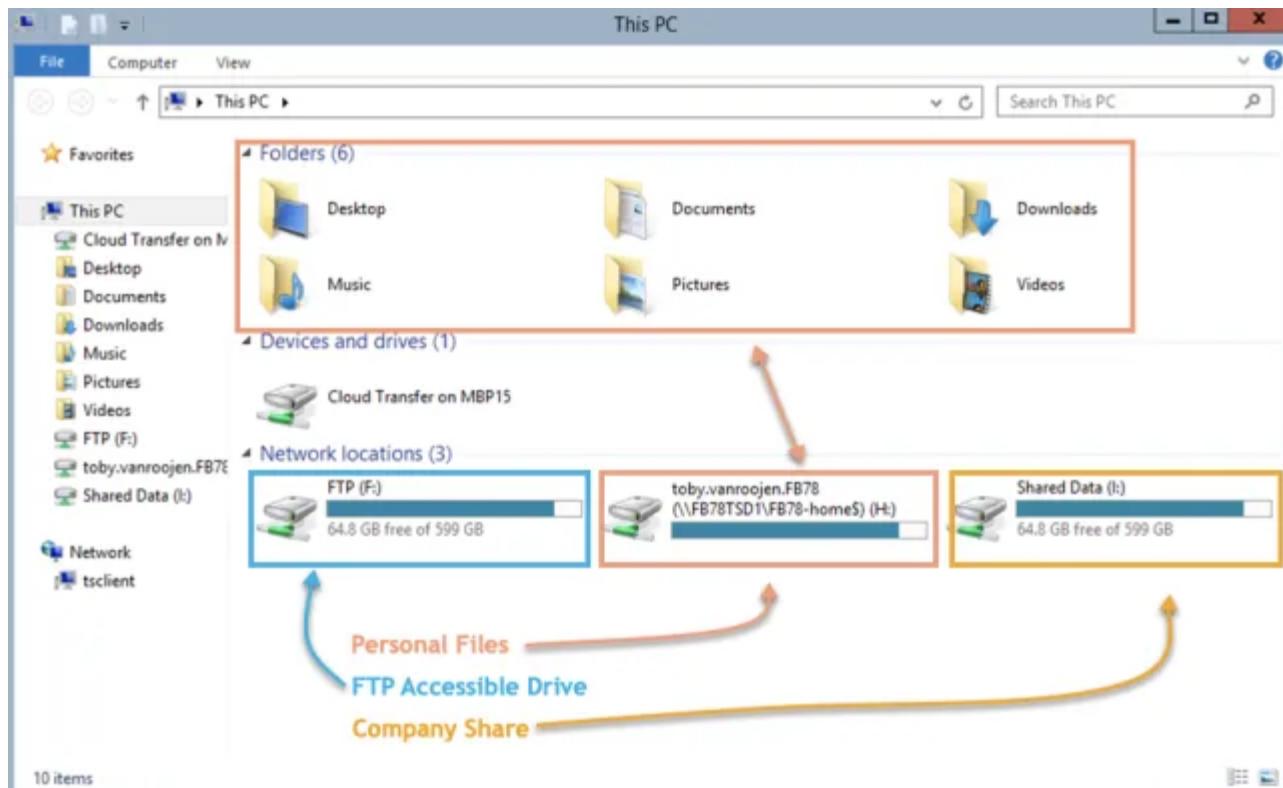
Managing Data Permissions

End user perspective

Virtual Desktop end users can have access to several mapped drives. These drives includes an FTPs accessible team share, a Company File Share and their Home drive (for their documents, desktop, etc...) . All of these mapped drives reference back to a central storage layer on either a storage services (such as Azure NetApp Files) or on a file server VM.

Depending on the configuration the user may or may not have the H: or F: drives exposed, they may only see their Desktop, Documents, etc... folders. Additionally, different Drive letters are occasionally set by the VDS administrator at deployment.





Managing permissions

VDS allows admins to edit security groups and folder permissions, all from within the VDS portal.

Security groups

Security groups are managed by clicking: Workspaces > Tenant Name > Users & Groups > under the Groups Section

In this section you can:

1. Create new security groups
2. Add/Remove users to the groups
3. Assign applications to groups
4. Enable/Disable Local Drive access to groups

Folder permissions

Folder Permissions are managed by clicking: Workspaces > Tenant Name > Manage (in the Folders section).

In this section you can:

1. Add/Delete Folders
2. Assign permissions to user or groups
3. Customize permissions to Read Only, Full Control & None



Application Entitlement

Overview

VDS has a robust application automation and entitlement functionality built-in. This functionality allows users to have access to different applications while connecting to the same session host(s). This is accomplished by some custom GPOs hiding shortcuts along with automation selectively placing shortcuts on the users' desktops.



This workflow only applies to RDS deployments. For AVD application entitlement documentation, please see [Application Entitlement Workflow for AVD](#)

Applications can be assigned to users directly or via Security groups managed in VDS.

At a high level, the application provisioning process follows these steps.

1. Add App(s) to App Catalog
2. Add App(s) to the workspace
3. Install the Application on all Session Hosts
4. Select the Shortcut path
5. Assign apps to users and/or groups



Steps 3 & 4 can be fully automated with Scripted Events as illustrated below



NetApp Virtual Desktop Service

Application Management

Toby vanRoojen
Product Marketing Manager
June, 2020

Video Walkthrough

Add applications to the App Catalog

VDS Application Entitlement starts with the App Catalog, this is a listing of all the applications available for deployment to end user environments.

To add applications to the catalog, follow these steps

1. Log in to VDS at <https://manage.cloudworkspace.com> using your primary admin credentials.
2. In the upper right, click the arrow icon next to your User Name and select Settings.
3. Click the App Catalog tab.
4. Click the Add App option in the Application Catalog title bar.
5. To add a group of applications, choose the Import Apps option.
 - a. A dialog will appear that provides an Excel template to download that creates the correct format for the application list.
 - b. For this evaluation NetApp VDS has created a sample application list for import it can be found [here](#).
 - c. Click on the Upload area and choose the application template file, click the Import button.
6. To add individual applications, choose the Add App button and a dialog box will appear.
 - a. Enter the name of the application.
 - b. External ID can be used to enter an internal tracking identifier such as a product SKU or billing tracking code (optional).
 - c. Check the Subscription box if you want to report on the applications as a Subscription product (optional).
 - d. If the product does not install by version (for example Chrome) check the Version Not Required checkbox. This allows “continuous update” products to be installed without tracking their versions.

- e. Conversely, if a product supports multiple named versions (ex: Quickbooks) you need to check this box so that you can install multiple versions and have VDS specific each available version in the list of applications that can be entitled for and end user.
- f. Check “No User Desktop Icon” if you don’t want VDS to provision a desktop icon for this product. This is used for “backend” products like SQL Server since end users don’t have an application to access.
- g. “App Must be Associated” enforces the need for an associated app to be installed. For example, a client server application may require SQL Server or mySQL to be installed as well.
- h. Checking the License Required box indicates that VDS should request a license file to be uploaded for an installation of this application before it sets the application status to active. This step is performed on the Application detail page of VDS.
- i. Visible to All – application entitlement can be limited to specific subpartners in a multi-channel hierarchy. For evaluation purposes, click the Check Box so that all users can see it in their available application list.

Add the application to the Workspace

To start the deployment process you’ll add the app to the workspace.

To do this, follow these steps

1. Click Workspaces
2. Scroll down to Apps
3. Click Add
4. Check box the application(s), enter required information, click Add Application, click Add Apps.

Manually install the application

Once the application has been added to the Workspace you’ll need to get that application installed on all session hosts. This can be done manually and/or it can be automated.

To manually install applications on session hosts, follow these steps

1. Navigate to Service Board.
2. Click on the Service Board Task.
3. Click on the Server Name(s) to connect as a local admin.
4. Install the app(s), confirm the shortcut to this app is found in the Start Menu path.
 - a. For Server 2016 and Windows 10: C:\ProgramData\Microsoft\Windows\Start Menu\Programs.
5. Go back to the Service Board Task, click Browse and choose either the shortcut or a folder containing shortcuts.
6. Whichever you select is what will be displayed on the end user desktop when assigned the app.
7. Folders are great when an app is actually multiple applications. e.g “Microsoft Office” is easier to deploy as a folder with each app as a shortcut inside the folder.
8. Click Complete Installation.
9. If required, open the created Icon Add Service Board Task and confirm the icon has been added.

Assign applications to users

Application entitlement is handled by VDS and application can be assigned to users in three ways

Assign Applications to Users

1. Navigate to the User Detail page.
2. Navigate to the Applications section.
3. Check the box next to all applications required by this user.

Assign users to an application

1. Navigate to the Applications section on the Workspace Detail page.
2. Click on the name of the application.
3. Check the box next to the users the application.

Assign applications and users to user groups

1. Navigate to the Users and Groups Detail.
2. Add a new group or edit an existing group.
3. Assign user(s) and application(s) to the group.

Reset User Password

Reset user password steps

1. Navigate to the Used Detail page in VDS

The screenshot shows the 'TrainWVD2's Workspace (rs6a)' page in the Microsoft Cloud Adoption Toolkit. The left sidebar has a 'Workspaces' menu item highlighted with a blue arrow. The top navigation bar has a 'Users & Groups' tab highlighted with a blue arrow. The main content area shows a table of users:

Name	Username	Status	Connection Status
Toby vanRoojen	admin@trainwv...	Available	Offline
WVD User1	WVDUser1@tr...	Available	Offline

2. Find the Password Section, enter the new PW twice and click

The screenshot shows the CloudJumper Cloud Workspace interface. On the left, a sidebar lists navigation options: Dashboard, Organizations (selected), Deployments, Workspaces, App Services, Service Board (with a red notification badge), Scripted Events, Admins, and Reports. The main content area displays user details for 'WVD User1' (WVDUser1@trainwvd2.onmicrosoft.com). The 'Overview' tab is selected, showing basic information like Username (WVDUser1), Connection Status (Offline), and Status (Available). Below this is a 'Security Settings' section with checkboxes for VDI User Enabled, Account Expiration Enabled, Force Password Reset at Next Login, Multi-factor Auth Enabled, Mobile Drive Enabled, Local Drive Access Enabled, Wake On Demand Enabled, and Admin Access Enabled (which is checked). A large black arrow points from the top-left towards the 'Update' button. A smaller black box highlights the 'Password Reset' section, which contains fields for 'Password' and 'Confirm Password', both filled with '*****'. A black arrow points to the 'Reset Password' button.

Time to take effect

- For environments running an “Internal” AD on VMs in the environment the password change should take effect immediately.
- For environments running Azure AD Domain Services (AADDS) the password change should take about 20 minutes to take effect.
- The AD type can be determined on the Deployment Details Page:

The screenshot shows the Cloud Workspace interface. On the left, there's a sidebar with icons for Dashboard, Organizations, Deployments (which is highlighted with a red arrow), Workspaces, App Services, Service Board (with a red notification badge), Scripted Events, Admins, and Reports. The main content area is titled 'All Deployments' for 'trainwvd2.onmicrosoft.com (kjd)'. It has tabs for Overview, Resource Defaults, Backup Defaults, and Provisioning Collections. Under Overview, there's a 'Deployment Details' card for 'trainwvd2.onmicrosoft.com' with fields like Description (kjd), Deployment Code (kjd), Version (5.3), Hypervisor (Azure), Resource Allocation Type (Domain), MachineSize (trainwvd2.onmicrosoft.com), h5 Gateway (kjd-h5gw.kjd.cloudworkspace.app:444), RDP Gateway (kjd-rds.kjd.cloudworkspace.app), and FTP Server Address (kjd-ftp.kjd.cloudworkspace.app). Below this is a 'Platform Servers' table with one entry: CWMGR1 (2 CPU, 4 RAM, Online status). At the bottom is a 'Platform Processes' table with several entries: New Client (Idle), Update Client (Idle), Delete Client (Idle), Server Cache (Idle), New User (Idle), Update User (Idle), Delete User (Idle), New App Service (Idle), Update App Service (Idle), and Delete App Service (Idle). A 'Refresh' button is at the top right of the processes table.

Self service password reset (SSRP)

The NetApp VDS Windows client and the NetApp VDS web client will provide a prompt for users that enter an incorrect password when logging into a v5.2 (or later) virtual desktop deployment. In the event that the user has locked their account, this process will unlock a user's account as well.

Note: users must have already entered a mobile phone number or an email address for this process to work.

SSPR is supported with:

- NetApp VDS Window Client
- NetApp VDS Web Client

In this set of instructions, you will walk through the process of using SSPR as a simple means to enable users to reset their passwords and unlock their accounts.

NetApp VDS Windows client

1. As an end user, click the Forgot Password link to continue.



Welcome to Cloud Workspace®

Sign into your workspace

Please check your username and password and try again.

Username

recording@wvdrecording.onmicrosoft.com

Password

••••••••

[Forgot Password](#)

Save Username

[Sign In](#)

2. Select whether to receive your code via your mobile phone or via email.



Welcome to Cloud Workspace®

Sign into your workspace

Username

recording@wvdrecording.onmicrosoft.com

Send Code Using:

Email

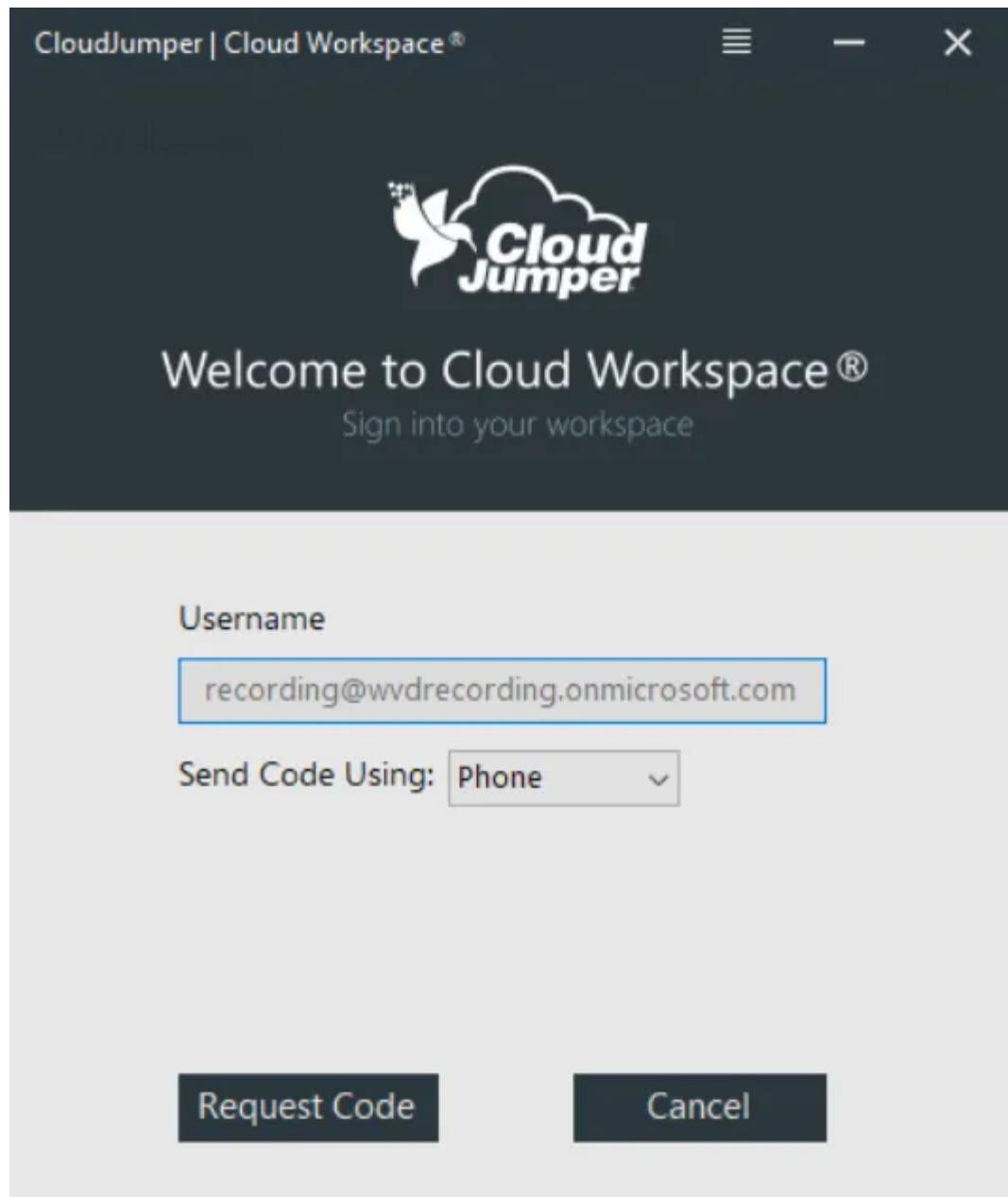
Email

Phone

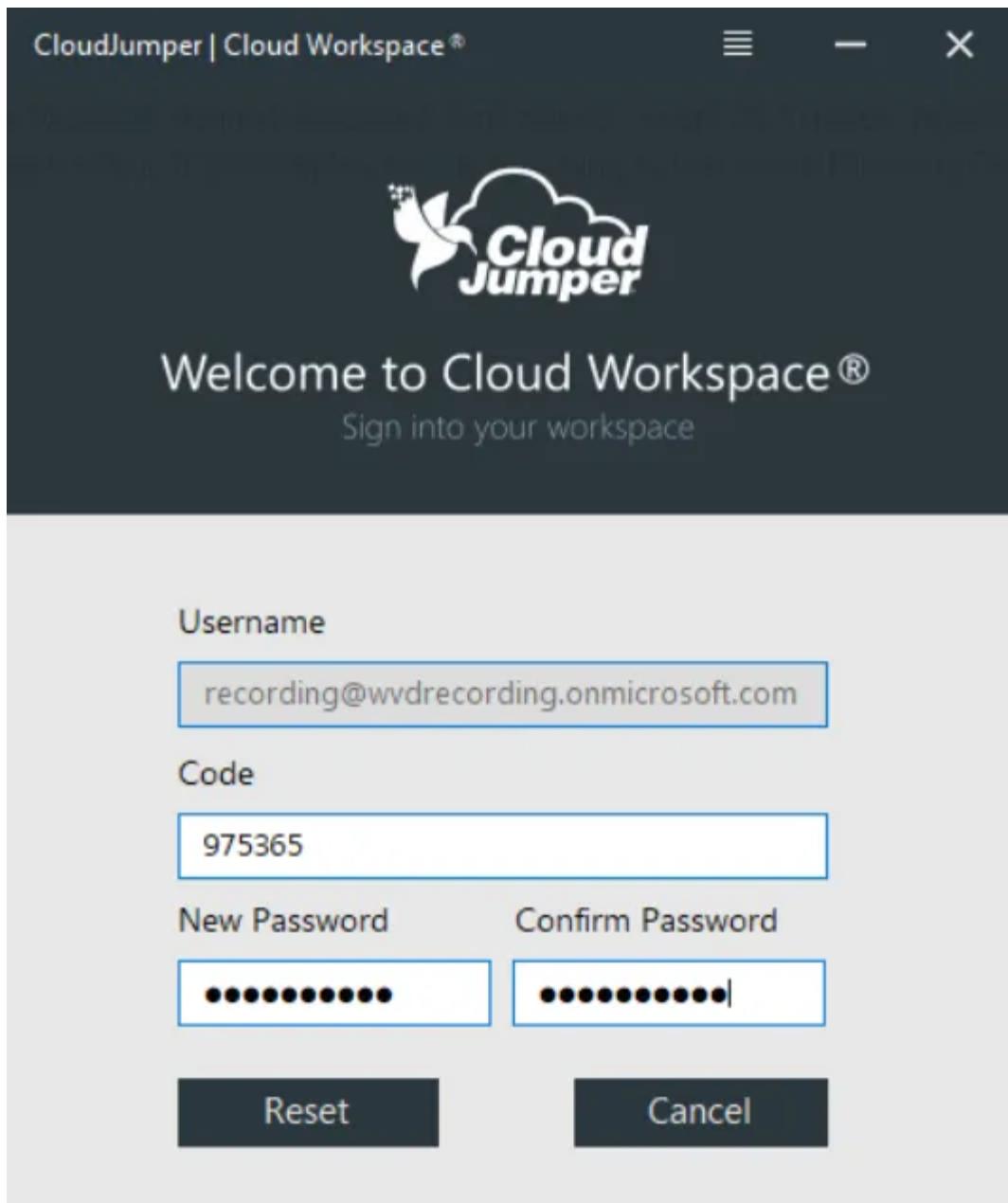
Request Code

Cancel

3. If an end user has only provided one of those contact methods, that will be the only method displayed.



4. After this step, users will be presented with a Code field where they should enter the numeric value received either on their mobile device or in their inbox (depending which was selected). Enter that code followed by the new password and click Reset to proceed.



5. Users will see a prompt informing them that their password reset has been completed successfully – click Done to proceed to complete the logon process.



If your deployment is using Azure Active Directory Domain Services, there is a Microsoft-defined password sync period – every 20 minutes. Again, this is controlled by Microsoft and cannot be changed. With this in mind, VDS displays that the user should wait for up to 20 minutes for their new password to take effect. If your deployment is not using Azure Active Directory Domain Services, the user will be able to log in again in seconds.



Welcome to Cloud Workspace®

Sign into your workspace

Your password has been reset successfully.

Please allow up to 20 minutes before using the new password to login.

Username

Code

New Password

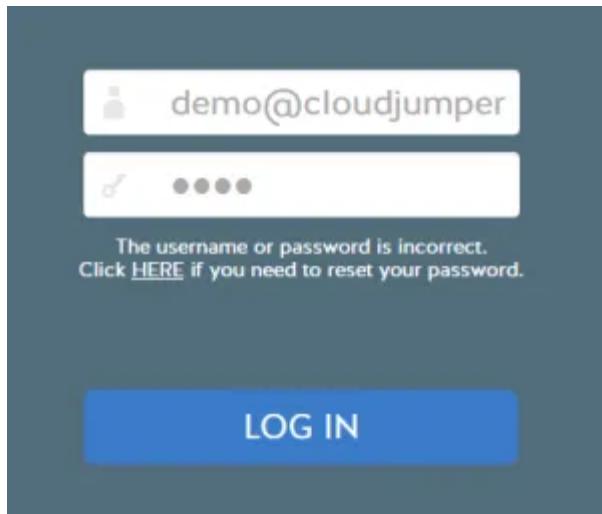
Confirm Password

Reset

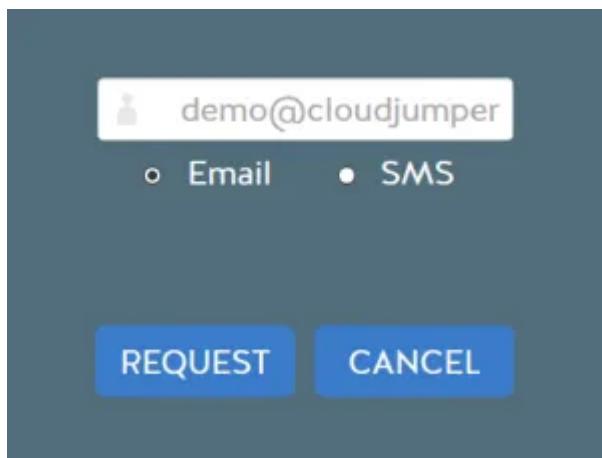
Done

HTML5 portal

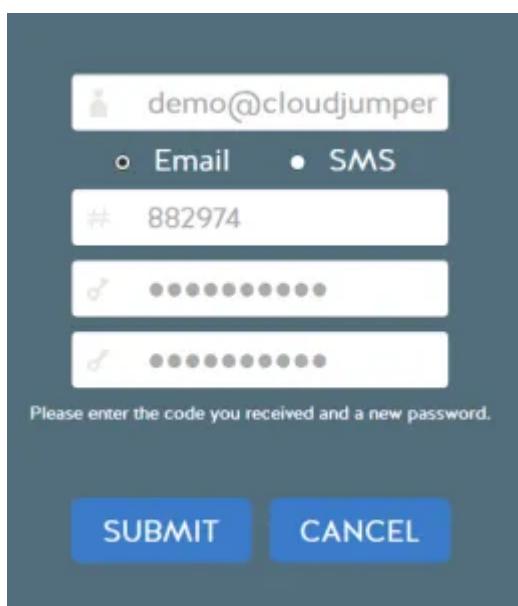
1. If the user fails to enter the correct password when attempting to login through the HTML5, they will now be presented with an option to reset the password:



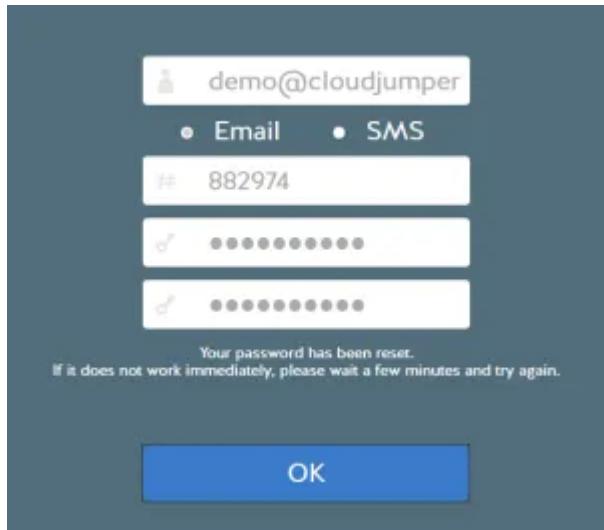
2. After clicking on the option to reset their password, they will be presented with their reset options:



3. The 'Request' button will send a generated code to the option selected (in this case the user's email). The code is valid for 15 minutes.



4. The password has now been reset! It is important to remember that Windows Active Directory will often need a moment to propagate the change so if the new password does not work immediately, just wait a few minutes and try again. This is particularly relevant for users residing in an Azure Active Directory Domain Services deployment, where a password reset could take up to 20 minutes to propagate.



Enabling self service password reset (SSPR) for users

To use Self Service Password Reset (SSPR), administrators must first enter a mobile phone number and/or an email account for an end user. There are two ways to enter a mobile number and email addresses for a virtual desktop user as detailed below.

In this set of instructions, you will walk through the process of configuring SSPR as a simple means for end users to reset their passwords.

Bulk importing users via VDS

Start by navigating to the Workspaces module, then Users & Groups and then clicking Add/Import.

You can enter these values for users when creating them one by one:

 Add User

First Name
 

Last Name

Username

Phone

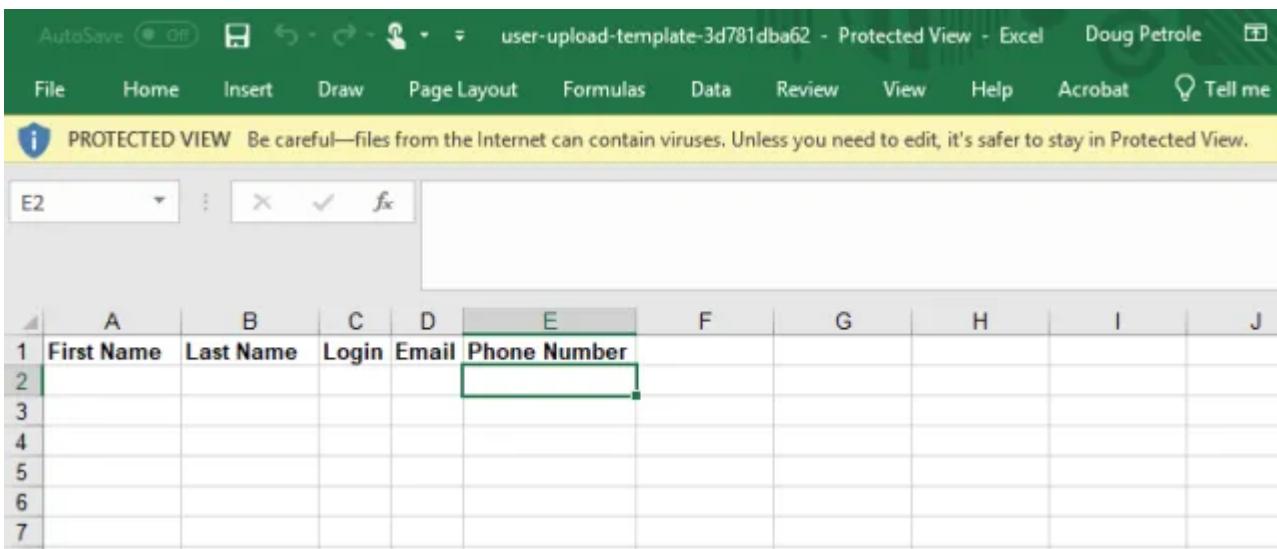
Email

Mobile Drive Enabled

Multi-Factor Auth Enabled

Local Drive Access Enabled

Or you can include these when bulk-importing users downloading and uploading the preconfigured Excel XLSX file in with this content filled out:



The screenshot shows a Microsoft Excel spreadsheet titled "user-upload-template-3d781dba62.xlsx". The ribbon menu includes AutoSave, Home, Insert, Draw, Page Layout, Formulas, Data, Review, View, Help, Acrobat, and Tell me. A yellow banner at the top reads "PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View." The spreadsheet has a header row with columns labeled A through J. Column A is "First Name", column B is "Last Name", column C is "Login", column D is "Email", and column E is "Phone Number". Row 1 contains the header labels, and row 2 contains the first data row. Rows 3 through 7 are empty.

A	B	C	D	E	F	G	H	I	J
1	First Name	Last Name	Login	Email	Phone Number				
2									
3									
4									
5									
6									
7									

Supplying the data via the VDS API

NetApp VDS API – specifically this call https://api.cloudworkspace.com/5.4/swagger/ui/index#!/User/User_PutUser – provides the ability to update this information.

Updating existing user phone

Update the users' phone number on the User Detail Overview page in VDS.

The screenshot shows the Cloud Jumper DEV WVD Cloud Workspace interface. The left sidebar has a blue header 'Cloud Jumper DEV WVD' and a 'Cloud Workspace' section. Below are navigation links: Dashboard, Organizations (which is selected and highlighted in blue), Data Centers, Workspaces, App Services, Service Board, Scripted Events, Admins, and Reports. The main content area shows a user overview for 'Doug Petrole (DPetrole@cjdevshivok1.com)'. The 'Overview' tab is selected. Under 'User Details', the 'Username' is listed as 'DPetrole'. There are fields for 'Phone' and 'Email' which are currently empty. The URL in the browser is 'Cloud Jumper DEV WVD(iva2)'.

Using other consoles

Note: you currently cannot provide a phone number for a user via the Azure Console, Partner Center or from the Office 365 Admin console.

Customize SSPR sending address

NetApp VDS can be configured to send the confirmation email *from* a custom address. This is a service provided to our service provider partners who wish for their end users to receive the reset password email to be sent from their own customized email domain.

This customization requires some additional steps to verify the sending address. To start this process, please open a support case with VDS support requesting a custom "Self Service Password Reset Source Address". Please define the following:

- Your partner code (this can be found by clicking on *settings* under the upper-right down arrow menu. See screenshot below)

- Desired "from" address (which must be valid)
- To which clients the setting should apply (or all)

Opening a support case can be done by emailing: VDSsupport@netapp.com

Once received, VDS support will work to validate the address with our SMTP service and activate this setting. Ideally you'll have the ability to update public DNS records on the source address domain to maximize email deliverability.

Password complexity

VDS can be configured to enforce password complexity. The setting for this is on the Workspace Detail Page in the Cloud Workspace Settings section.

Scroll down

Company Details		Contact Details	
Company Name TrainWVD2	Company Code rs6a	Primary Notification Email	Phone
Status Available	Partner CloudJumper CSP Master	Address 1	Address 2
Organization Type Client	Login Identifier @trainwvd2.onmicrosoft.com	City Garner	Zip Code
Created By	Deployment	State	Country

Available Organization Type Client

CloudJumper CSP Master Login Identifier @trainwvd2.onmicrosoft.com

Created By Deployment kjd

Website Server Address rs6a.kjd.cloudworkspace.app

Cloud Workspace Settings

App Settings

- Remote App Access Enable App Locker
- Enable Application Usage Tracking

Device Settings

- Disable Printing Access User Profile Disk
- User Data Storage Enable Task Manager

Security Settings

- Force Password Complexity File Auditing Enabled
- Migration Mode Enabled MFA for All Users Enabled

Account Options

- Account Lockout Notifications

Audit Reports

Report Select a Report

Apps

Add

Filter by Keyword

Name Status

Password complexity: Off

Policy	Guideline
Minimum Password Length	8 characters
Maximum Password Age	110 days
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lockout will occur after 5 incorrect entries
Lock Duration	30 minutes

Password complexity: On

Policy	Guideline
Minimum Password Length	<p>8 characters</p> <p>Not contain the user's account name or parts of the user's full name that exceed two consecutive characters</p> <p>Contain characters from three of the following four categories:</p> <ul style="list-style-type: none"> English uppercase characters (A through Z) English lowercase characters (a through z) Base 10 digits (0 through 9) Non-alphabetic characters (for example, !, \$, #, %) <p>Complexity requirements are enforced when passwords are changed or created.</p>
Maximum Password Age	110 days

Policy	Guideline
Minimum Password Age	0 days
Enforce Password History	24 passwords remembered
Password Lock	Automatically lock will occur after 5 incorrect entries
Lock Duration	Remains locked until administrator unlocks

Multi-Factor Authentication (MFA)

Overview

NetApp Virtual Desktop Service (VDS) includes an SMS/Email based MFA service at no additional charge. This service is independent of any other services (e.g. Azure Conditional Access) and can be used to secure administrator logins to VDS and user logins to virtual desktops.

MFA basics

- VDS MFA can be assigned to admin users, individual end users or applied to all end users
- VDS MFA can send SMS or Email notifications
- VDS MFA has a self-service initial setup and reset function

Guide scope

This guide walks you thru the setup of MFA along with an illustration of the end user experience

This guide covers the following subjects:

1. [Enabling MFA for Individual Users](#)
2. [Requiring MFA for All Users](#)
3. [Enabling MFA for Individual Administrators](#)
4. [End User Initial Setup](#)

Enabling MFA for individual users

MFA can be enabled for individual users on the user detail page by clicking *Multi-factor Auth Enabled*

Workspaces > Workspace Name > Users & Groups > User Name > Multi-factor Auth Enabled > Update

MFA can also be assigned to all users, if this setting is in place, the checkbox will be checked and (*via Client Settings*) will be appended to the checkbox label.

Requiring MFA for all users

MFA can be enabled and enforced across all users on the workspace detail page by clicking *MFA for All Users Enabled*

Workspaces > Workspace Name > MFA for All Users Enabled >Update

Enabling MFA for individual administrators

MFA is also available for administrator accounts accessing the VDS portal. This can be enabled per administrator on the admin detail page.

Admins > Admin Name > Multi-Factor Auth Required > Update

Initial setup

On the first login after enabling MFA, the user or admin will be prompted to enter an email address or mobile phone number. They'll receive a confirmation code to enter and confirm successful enrollment.

System Administration

Create a Domain Admin ("Level 3") Account

Overview

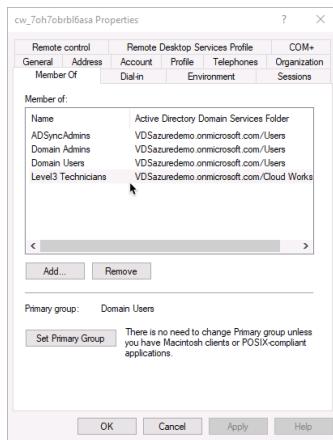
Occasionally VDS administrators will need domain-level credentials to manage the environment. In VDS these are called "Level 3" or ".tech" account.

These instructions show how these accounts can be created with the appropriate permissions.

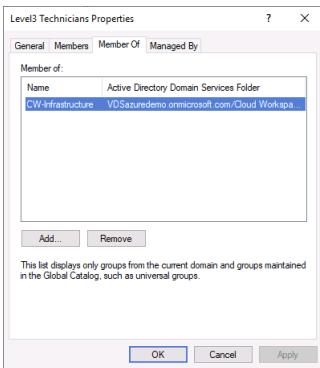
Windows Server Domain Controller

When running an internally hosted Domain Controller (or a local DC linked to Azure via a VPN/Express Route) managing .tech accounts can be done directly in Active Directory Manager.

1. Connect to the Domain Controller (CWMGR1, DC01 or the existing VM) with a domain admin (.tech) account.
2. Create a new user (if needed).
3. Add the user to the "Level3 Technicians" security group



- a. If the "Level3 Technicians" security group is missing, please create the group and make it a member of "CW-Infrastructure" security group.



Adding “.tech” to the end of the username is a recommended best practice to help delineate admin accounts from end user accounts.

Azure AD Domain Services

If running in Azure AD Domain Services or managing user in Azure AD, these accounts can be managed (i.e. password change) in the Azure Management Portal as a normal Azure AD user.

New accounts can be created, adding them to these roles should give them the permissions required:

1. AAD DC Administrators
2. ClientDHPAccess
3. Global Admin in the directory.



Adding “.tech” to the end of the username is a recommended best practice to help delineate admin accounts from end user accounts.

NAME	GROUP TYPE	MEMBERSHIP TYPE
AAD DC Administrators	Security	Assigned
ClientDHPAccess	Security	Assigned

Providing Temporary Access to 3rd Parties

Overview

Providing access to 3rd parties is a common practice when migrating to any cloud solution.

VDS Admins often elect to not give these 3rd parties the same level of access that they have, to follow a “least required” security access policy.

To set up admin access for 3rd parties, log into VDS and navigate to the Organizations module, click into the organization and click Users & Groups.

Next, create a new User account for the 3rd party and scroll down until you see the Admin Access section and check the box to enable admin rights.



The VDS Admin is then presented with the Admin Access setup screen. There is no need to change user's name, login or password – just add phone number and/or email if you want to enforce Multi-Factor Authentication and select the level of access to grant.

For database administrators like a VAR or ISV, Servers is commonly the only access module required.

New Active Directory Admin

Basic Info <p>Username <input type="text" value="UOne@gputesting.onmicrosoft.com"/></p> <p>First Name <input type="text" value="User"/></p> <p>Last Name <input type="text" value="One"/></p> <p>Phone Number <input type="text" value="Enter Phone #"/></p> <p>Email <input type="text" value="Enter Email"/></p>	Security Settings <p><input type="checkbox"/> Multi-Factor Auth Required</p> <p><input type="checkbox"/> Tech Account Enabled</p> <p><input type="checkbox"/> User Support Only</p> <p><input type="checkbox"/> Shadow User Enabled</p>	Module Permissions <p>Module <input checked="" type="checkbox"/></p> <p>Audits <input type="checkbox"/></p> <p>Applications <input type="checkbox"/></p> <p>Groups <input type="checkbox"/></p> <p>Firewall <input type="checkbox"/></p> <p>Folders <input type="checkbox"/></p> <p>Servers <input type="checkbox"/></p> <p>Users <input type="checkbox"/></p>
<input type="button" value="Cancel"/> <input type="button" value="Add Admin"/>		

Once saved, the End User gains access to self-management functions by logging into VDS with their standard Virtual Desktop user credentials.

When the newly created User logs in, they will only see the modules you have assigned to them. They can select the organization, scroll down to the Servers section and connect to the server name you tell them to (say, <XYZ>D1, where XYZ is your company code and D1 designates that the server is a Data server. In the example below, we would tell them to connect to the TSD1 server to perform their assignments.

Servers							Add	Refresh
Name	Type	Machine Size	RAM	CPU	Online Status	Status		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Power User	Standard_B2s	4 GB	2	● Online	● Available		
[REDACTED]	Shared	Standard_B2s	4 GB	2	● Online	● Available		

Configure Backup Schedule

Overview

VDS has the ability to configure and manage native backup services in some infrastructure providers including Azure.

Azure

In Azure, VDS can automatically configure backups using native [Azure Cloud Backup](#) with locally redundant

storage (LRS). Geo-redundant storage (GRS) can be configured in the Azure Management Portal if needed.

- Individual backup policies can be defined for each Server Type (with default recommendations). Additionally, individual machines can be assigned a schedule independent (from their server type) from within the VDS UI, this setting can be applied by navigating to the Server Detail View by clicking on the Server name on the Workspace page (See Video Below: Setting Individual Backup Policies)
 - Data
 - Backup with 7 daily, 5 weekly & 2 monthly backups. Increase retention periods based on business requirements.
 - This is true for both a dedicated Data server and for add-on VPS VMs for Apps and Databases.
 - Infrastructure
 - CWMGR1 – Backup Daily and keep 7 daily, 5 weekly, 2 monthly.
 - RDS Gateway – Backup weekly and keep 4 weekly.
 - HTML5 Gateway – Backup weekly and keep 4 weekly.
 - PowerUser (aka VDI User)
 - Don't backup the VM as data should be stored on a D1 or TSD1 server.
 - Be aware that some applications do store data locally and special considerations should be taken if this is the case.
 - In the event of a VM failure, a new VM can be built via Cloning another. In the event there is only one VDI VM (or one unique VM build) it is advisable to back it up so that a complete rebuild of that VM is not required.
 - If needed, rather than backing up all VDI servers, costs can be minimized by manually configuring a single VM to backup directly in the Azure Management portal.
 - TS
 - Don't backup the VM as data should be stored on a D1 or TSD1 server.
 - Be aware that some applications do store data locally and special considerations should be taken if this is the case.
 - In the event of a VM failure, a new VM can be built via Cloning another. In the event there is only one TS VM it is advisable to back it up so that a complete rebuild of that VM is not required.
 - If needed, rather than backing up all TS servers, costs can be minimized by manually configuring a single VM to backup directly in the Azure Management portal.
 - TSData
 - Backup with 7 daily, 5 weekly & 2 monthly backups. Increase retention periods based on business requirements.
- Policies can be set to take backups daily or weekly, Azure does not support more frequent schedules.
- For daily schedules, enter the preferred time to take the backup. For weekly schedules, enter the preferred day and time to take the backup. Note: Setting the time to exactly 12:00 am can cause issues in Azure Backup so 12:01 am is recommended.
- Define how many daily, weekly, monthly and yearly backups should be retained.

Setting deployment defaults

In order to setup Azure backup for the entire deployment, follow these steps:

1. Navigate to the Deployments detail page, select Backup Defaults
2. Select a server type from the drop-down menu. The server types are:

Data: these are for LOB/database server types

Infrastructure: these are platform servers

Power User: these are for Users with a TS server dedicated solely to them

TS: these are terminal servers that Users launch sessions on

TSData: these are servers doubling as terminal and data servers.

- This will define the overarching backup settings for the entire Deployment. These can be overridden and set at a server-specific level later if desired.
3. Click the settings wheel, then the Edit popup that appears.
 4. Select the following backup settings:

On or off

Daily or weekly

What time of day backups take place

How long each backup type (daily, weekly, etc.) should be retained

5. Finally, click Create (or Edit) Schedule to put these settings in place.

Setting individual backup policies

To apply server-specific integrated backup settings, navigate to a Workspace detail page.

1. Scroll down to the Servers section and click on a server's name
2. Click Add Schedule
3. Apply backup settings as desired and click Create Schedule

Restoring from backup

To restore backups of a given VM, begin by navigating to that Workspace detail page.

1. Scroll down to the Servers section and click on a server's name
2. Scroll down to the Backups section and click the wheel to expand your options, then select either
3. Restore to Server or Restore to Disk (attach a drive from the backup so that you can copy data from the backup to the existing version of the VM).
4. Proceed with your restore from this point on as you would in any other restore scenario.



Costs depend on what schedule you want to maintain and is entirely driven by the Azure backup cost. Backup pricing for VMs is found on the Azure Cost Calculator: <https://azure.microsoft.com/en-us/pricing/calculator/>

Cloning Virtual Machines

Overview

Virtual Desktop Service (VDS) provides the ability to clone an existing virtual machine (VM). This functionality designed to automatically increase server unit count availability as defined user count grows OR additional servers to available resource pools.

Admins use cloning in VDS in two ways:

1. On demand automated creation of new server from an existing client server
2. Proactive automated creation of new client server(s) for auto-scaling of resources based-on rules defined and controlled by partners

Cloning to add additional shared servers

A clone is a copy of an existing virtual machine. Cloning functionality saves time and helps admins scale because installing a guest operating system and applications can be time consuming. With clones, you can make many copies of a virtual machine from a single installation and configuration process. This typically looks like:

1. Install all desired applications and settings onto a TS or TSD server
2. Navigate to: Workspaces > Servers Section > Gear Icon for the Source Server > Click Clone
3. Allow the clone process to run (typically 45-90 minutes)
4. The final step activate the cloned server, putting it into the RDS pool to accept new connections. Cloned servers may require individual configuration after being cloned so VDS waits for the Administrator to manually put the server into rotation.

Repeat as many times as necessary.



To increase the capacity for users in a shared session host environment, cloning a session host is an easy process requiring only a few steps.

1. Select a session host to clone, verify no users are currently logged in to the machine.
2. In VDS, navigate to the Workspace of the target client. Scroll to the Servers section, click the Gear Icon and select Clone. This process takes significant time and will take the source machine offline. Expect 30+ minutes to complete.

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Connect
DVYTS1	Shared	Standard_B2s	4 GB	2	● Online	● Convert To Data

Firewall Rules
No Rules Added.

Add Refresh

Filter by Keyword

Clone

Stop

Delete

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	0 GB	0	● Offline	○ In Progress (Cloning)
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

- The process will shut down the server, clone the server to another image and SysPrep the image to the next TS# for the customer. The server shows as *Type=staged* and *Status=Activation Required* in the Servers list.

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

- Logon to the server and verify that the server is ready for production.

Servers

Add Refresh

Filter by Keyword

Name	Type	Machine Size	RAM	CPU	Online Status	Status
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available

Firewall Rules

Add

No Rules Added.

Connect

Activate

Clone

Stop

Delete

- When ready, click Activate to add the server into the session-host pool to start accepting user connections.

Servers							Add	Refresh
							<input type="text"/> Filter by Keyword	
Name	Type	Machine Size	RAM	CPU	Online Status	Status		
DVYTS1	Power User	Standard_B2s	4 GB	2	● Online	● Available	Connect	
DVYTS2	Shared	Standard_B2s	4 GB	2	● Online	● Available	Activate	
DVYTS3	Staged	Standard_DS2_v2	7 GB	2	● Online	Activation Required	Clone	
DVYTSD1	Shared	Standard_B2s	4 GB	2	● Online	● Available	Stop	

Firewall Rules

No Rules Added.

Connect Activate Clone Add Stop Delete

VDS cloning process definition

The step-by-step process is detailed in VDS > Deployment > Task History under any Clone Server operations. The process has 20+ steps, which start with accessing the hypervisor to start the clone process & ends with activating the cloned server. The cloning process includes key steps such as:

- Configure DNS & set server name
- Assign StaticIP
- Add to Domain
- Update Active Directory
- Update VDS DB (SQL instance on CWMGR1)
- Create Firewall rules for the clone

As well as Task History, the detail steps for any cloning process can be viewed in CwVmAutomationService log on CWMGR1 in each partner's Virtual Desktop Deployment. Reviewing these log files is documented [here](#).

Automated creation of new server(s)

This VDS functionality designed to automatically increase server unit count availability as defined user count grows.

The partner defines and manages via VDS (<https://manage.cloudworkspace.com>) > Client > Overview – VM Resources > Auto-Scaling. Several controls are exposed to allow partners to Enable/Disable Auto Scaling as well as create custom rules for each client such as: number/users/server, additional RAM per user & number of users per CPU.



Above assumes automated cloning is enabled for the entire Virtual Desktop Deployment. For example, to stop all automated cloning, use DCConfig, in the Advanced window, uncheck the Server Creation→Automated Cloning Enabled.

When does the automated clone process run?

The automated clone process runs when the daily maintenance is configured to run. The default is midnight, but this can be edited. Part of the daily maintenance is to run the Change Resources thread for each resource pool. The Change Resources thread determines the number of shared servers required based-on the number of users the pool's configuration (customizable; can be 10, 21, 30, etc users per server).

“On demand” automated creation of new server

This VDS functionality allows automated “on demand” cloning of additional servers to available resource pools.

The VDS Admin logs into VDS and under the Organizations or Workspaces Modules, finds the specific Client & opens the Overview tab. The Servers Tile lists all servers (TSD1, TS1, D1, etc). To clone any individual server, simply click on the cog to far-right of server name & select Clone option.

Typically, the process should take about an hour. However, the duration depends on the size of VM and the available resources of the underlying hypervisor. Please note the server being cloned will need to be rebooted, so partners typically perform after hours or during a scheduled maintenance window.

When cloning a TSDData server, one of the steps is deleting the c:\Home, c:\Data, and c:\Pro folders so they’re aren’t any duplicate files. In this case, the clone process failed there were problems deleting these files. This error is vague. Typically, this means the clone event failed because there was an open file or process. Next attempt, please disable any AV (because that might explain this error).

Auto-increase Disk Space Feature

Overview

NetApp recognizes the need to give Administrators an easy way to make sure that users always have space to access and save documents. This also ensures that VMs have enough free space to complete backups successfully, enabling and empowering Administrators and their Disaster Recovery and Business Continuity plans. With this in mind, we built a feature that automatically expands the managed disk in use to the next tier when a drive is running short on space.

This is a setting that is applied by default on all new VDS deployments in Azure, ensuring that all deployments protect users and the tenant’s backups by default.

Administrators can validate this is in place by navigating to the Deployments tab, then selecting a deployment and then connecting to their CWMGR1 server from there. Next, open the DCConfig shortcut on the desktop and click Advanced and scroll down to the bottom.

The screenshot shows the DCConfig v5.2.19101.1441 - [Program Configuration] window. The 'Program' dropdown is set to 'CwVmAutomationService'. The main table lists various properties under different group names. The 'Automatically Expand Drive' property is highlighted with a red border and has its checkbox checked. Other properties include GroupName, FriendlyName, and Value columns.

GroupName	FriendlyName	Value
PEN	Logo	cloudworkspace-logo-med.png
PEN	NumNotifyDays	6
PEN	NotificationDay1	12
PEN	NotificationDay2	5
PEN	NotificationDay3	4
PEN	NotificationDay4	3
PEN	NotificationDay5	2
PEN	NotificationDay6	1
Monitoring	Enabled	<input checked="" type="checkbox"/>
Monitoring	Alert Server Down for Minutes	2
Monitoring	Alert Ram High for Minutes	60
Monitoring	Ram High %	95
Monitoring	Alert Cpu High for Minutes	60
Monitoring	CPU High %	95
Monitoring	Upload Data Every X Minutes	15
Delete Xml Delay	Minutes	90
Automatically Expand Drive	Enabled	<input checked="" type="checkbox"/>
Pci v3 Compliant	Enabled	<input type="checkbox"/>
Run CwAgent as Domain Admin	Enabled	<input checked="" type="checkbox"/>
Install WildCard Cert	On Infrastructure Servers	<input checked="" type="checkbox"/>

Administrators can change the amount of free space desired in either GB free or percent of the drive that

should be free before moving to the next tier of managed disks in the same Advanced section of DCCConfig.

FreeSpaceReport	MinFreeSpaceGB	10
FreeSpaceReport	MinFreeSpacePercent	10
MaxRebootTimeSpanHours	ClientServers	360

A few practical application examples:

- If you want to ensure that at least 50 GB is available on your drive, set MinFreeSpaceGB to 50
- If you want to ensure that at least 15% of your drive is free, set MinFreeSpacePercent from 10 to 15.

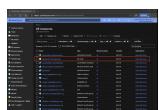
This action takes place at midnight on the server's time zone.

Accessing VDS credentials in Azure Key Vault

Overview

CWASetup 5.4 is a departure from previous Azure deployment methods. The configuration and validation process is streamlined to reduce the amount of information required to begin a deployment. Many of those removed prompts are for credentials or accounts such as Local VM Admin, SMTP account, Tech account, SQL SA, etc. These accounts are now automatically generated and stored in an Azure Key Vault. By default, accessing these automatically generated accounts requires an additional step, described below.

- Find the 'Key vault' resource and click into it:



- Under 'Settings', click 'Secrets'. You'll see a message stating that you are unauthorized to view:



- Add an 'Access Policy' to grant an Azure AD account (like a Global Admin or System Administrator) access to these sensitive keys:



- A Global Admin is used in this example. After selecting the principal, click 'Select', then 'Add':



- Click 'Save':



- Access policy has been successfully added:



- Revisit the 'Secrets' to verify the account now has access to the deployment accounts:



- For example, if you required the Domain Administrator credential to login to CWMGR1 and update Group Policy, check the strings under cjDomainAdministratorName and cjDomainAdministratorPassword by clicking on each entry:



- Show or Copy the value:



Apply Monitoring and Antivirus

Overview

Virtual Desktop Service (VDS) Administrators are responsible for monitoring both their platform infrastructure (which will consist of CWMGR1 at minimum) and all other infrastructure and virtual machines (VMs). In most cases, Administrators arrange infrastructure (hypervisor/SAN) monitoring directly with their Data Center/IaaS provider. Administrators are responsible for monitoring terminal servers and data servers, typically by deploying their preferred Remote Management and Monitoring (RMM) solution.

Anti-Virus is the responsibility of the administrator (for both platform infrastructure and terminal/data server VMs). To streamline this process, VDS for Azure servers have Windows Defender applied by default.



When installing 3rd party solutions, be sure not to include Firewalls or any other components which might interfere with VDS automation.

More specifically, when very specific Anti-Virus policies are in place by default this can result in adverse effects when these Anti-Virus agents are installed on a server managed by Virtual Desktop Service.

Our overall guidance is that while VDS platform automation is generally not impacted by Anti-Virus or Anti-Malware products, it is a best practice to add exceptions/exclusions for the following processes on all platform servers (CWMGR1, RDGateways, HTML5Gateways, FTP, etc):

```
*\paexec.exe  
*\paexec_1_25.exe  
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe  
C:\Program Files\CloudWorkspace\CW Automation  
Service\cw.automation.service.exe  
C:\Program  
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe  
C:\Program Files (x86)\Myrtle\bin\Myrtle.Printer.exe  
C:\Program Files (x86)\Myrtle\bin\Myrtle.Services.exe
```

Additionally, we recommend safe-listing the following processes on client servers:

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe  
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe  
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe  
C:\Program Files\CloudWorkspace\Pen\Pen.exe  
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe  
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

Adding and Moving Mapped Drives

Overview

By default there are three shared folders exposed to end user sessions. These folders are found on the defined storage layer. This could be on the file server (TSD1 or D1) or a storage service such as Azure Files, Azure NetApp Files, NetApp CVO and NetApp CVS.

To assist with clarity, this article will use an example customer with the company code “NECA.” This example assumes a single TDS1 server has been deployed, named NECATSD1. We’ll work through the process of moving a folder to another VM (Named “NECAD1”). This strategy can be used to move between partition on the same machine or to another machine as shown in the following example...

Folders Starting Location:

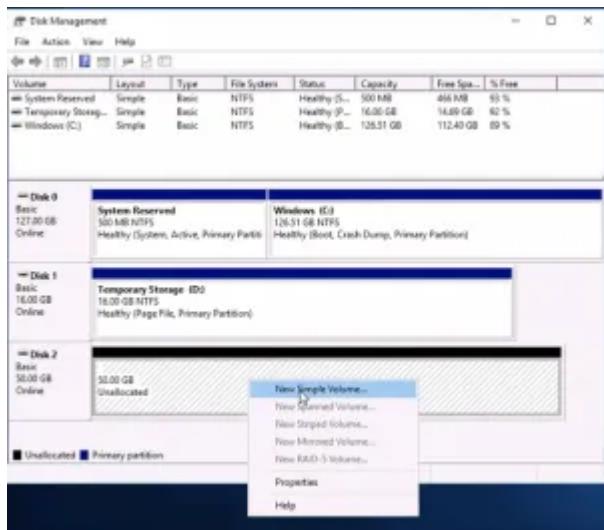
- Data: NECATSD1\C:\data\NECA\ (TSD1 means it is the first Terminal Server and also functions as the Data Server)
- FTP: NECATSD1\C:\ftp\NECA\
- Home: NECATSD1\C:\home\NECA\

Folders Ending Location:

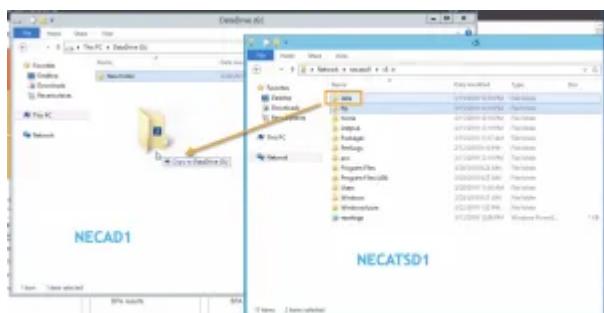
- Data: NECAD1\G:\data\NECA\ (the D1 means it is the 1st Data Server)
- FTP: The same process applies, no need to describe it 3x
- Home: The same process applies, no need to describe it 3x

Add disk for G: on NECAD1

1. In order to put the shared folder on the E: drive we'll need to add one via the hypervisor (e.g. Azure Management Portal), then initialize and format it

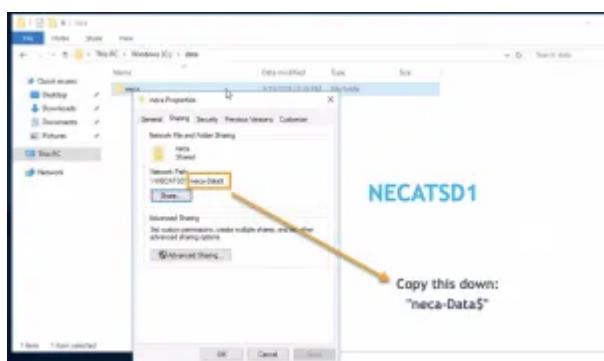


2. Copy the existing folder (on NECATSD1, C:\) path to the new location (on NECAD1, G:\)
3. Copy the folder(s) from the original location to the new location.

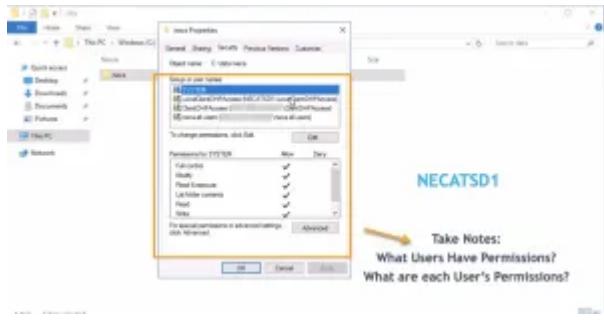


Gather Information From the Original Folder Share (NECATSD1, C:\data\NECA)

1. Share the new folder using the exact same path as the folder in the original location.
2. Open the new NECAD1, G:\data\ folder and you'll see a folder named the company code, "NECA" in our example.



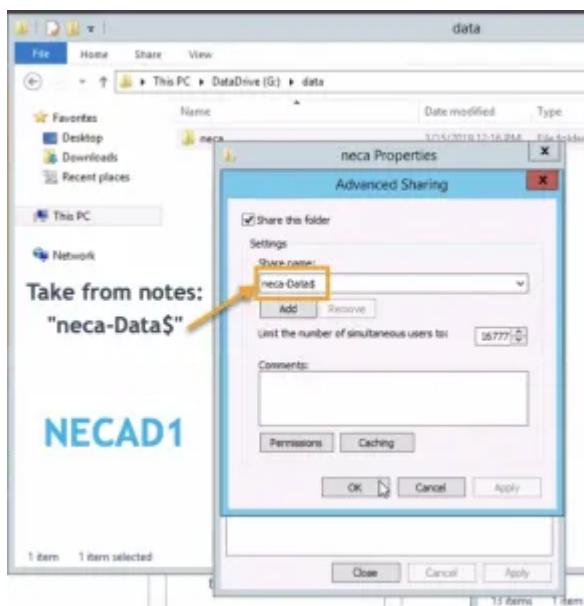
3. Note the security permissions of the original folder share:



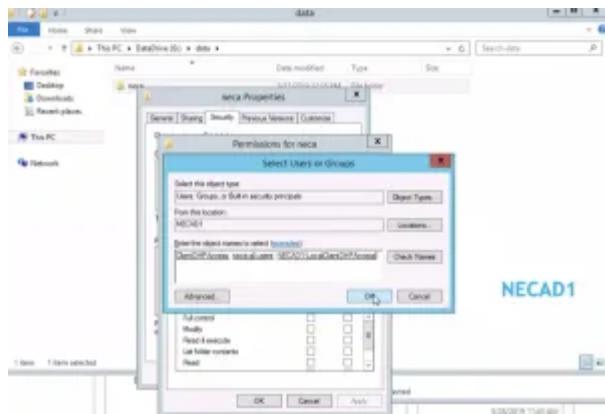
4. Here is the typical setup, however it is important to copy the original settings in case there are existing customizations we need to preserve. All other user/group permissions should be removed from the new folder share
- SYSTEM:All permissions allowed
 - LocalClientDHPAccess (on the local machine):All permissions allowed
 - ClientDHPAccess (on the domain): All permissions allowed
 - NECA-all users (on the domain): All permissions except “Full Control” allowed

Replicate the Sharing Path and Security Permissions to the New Shared Folder

1. Go back to the new location (NECAD1, G:\data\NECA\) and share the NECA folder with the same network path (excluding the machine), in our example “neca-data\$”

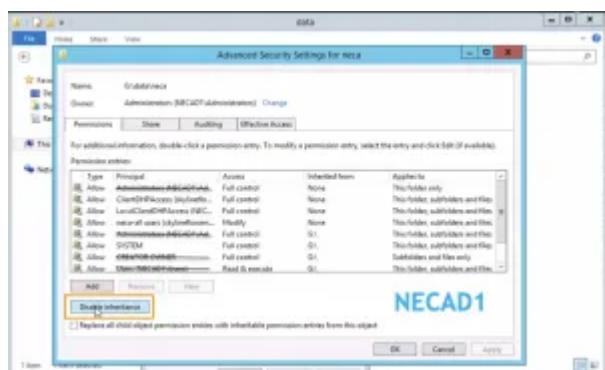


2. For user security add all the users, set their permissions to match.



NECAT1

3. Remove any other user/group permissions that may already exist.

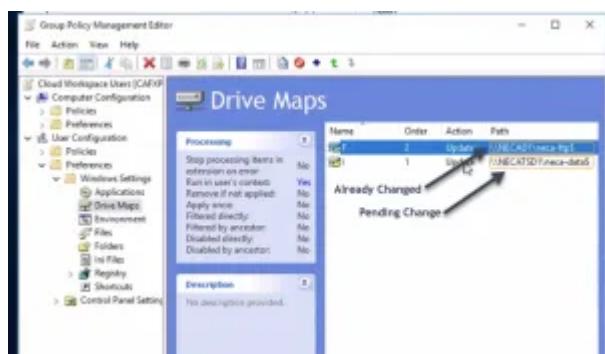


NECAT1

Edit Group Policy (Only if the folder moved to a new Machine)

1. Next you'll edit the Drive Maps in Group Policy Management Editor. For Azure AD Domain Services, the mapping is located in:

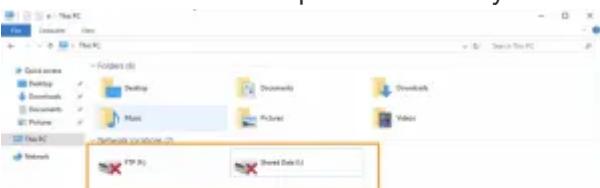
"Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps"



2. Once Group Policy updates, the next time each user connects, they'll see the mapped drives which are pointed back to the new location.
3. At this point you can delete the original folders, on NECATSD1, C:\.

Troubleshooting

If the end user sees the mapped drives with a red X, right click the drive and select disconnect. Log out and back in the drive will be present correctly.



Copyright Information

Copyright © 2021 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.