



Nerdio NME-200 Certification Exam Curriculum

Last Revised: May 2025

Table of Contents

Copyright	12
Introduction	13
About Nerdio Manager	14
Directory and identity management	16
Entra ID - definition of terms	16
Customers With a Cloud-Only Environment	17
Customers With Existing Servers and Applications and/or Virtual Desktops	17
Enable Active Directory Functionality in Azure	17
Do-it-yourself AD in Azure	18
Azure Active Directory Domain Services (AAD DS) PaaS	18
Configure Entra Domain Services for use with AVD	21
Preliminary Considerations	21
Entra Domain Services Design Principals	22
Create an Entra Domain Services Domain	23
Configure Nerdio Manager for Entra Domain Services	25
Installation and Getting Started	27
Nerdio Manager Installation Guide	27
Companion Video	27
Prerequisites	27
Install Nerdio Manager from the Azure Marketplace	28
Initialize Nerdio Manager	29
Configure Nerdio Manager Settings	31

Nerdio Manager Edition Management	36
Update the Nerdio Manager application	37
Nerdio Manager updates FAQs	38
Method 1: Deploy button	38
Method 2: Use Azure Cloud Shell (v2.10+)	39
Method 3: Standalone PowerShell update	40
Method 4: Manual "Zip Push" deployment	40
Method 5: Manual Azure Cloud Shell deployment	44
Restore Nerdio Manager to a previous version	46
Nerdio Manager Default Deployment Resources and Costs	47
Setup and Settings	48
Harden Nerdio Manager	48
Harden App Service	51
Harden Azure Storage Account	54
Harden SQL	59
Back up and restore Nerdio Manager configuration	61
Post-February 2025: Updated backup strategy	61
Prerequisites	62
App Service automatic backups	63
App Service custom backups	63
SQL Server backups	65
Key Vault backup	65
Key Vault restore	66
Pre-February 2025: Legacy backup strategy	68

Alerts and notifications	75
Create a new Intune alert condition	75
Cloud PC alert conditions	76
Create a new Nerdio Manager alert condition	77
Examples of conditions	79
Create a new action	81
Configure Azure Monitor Alerts for AVD Resources	83
Resource Selection Rules Management	86
Create a Resource Selection Rule	87
Manage Resource Selection Rules	90
Manage Schedules for Tasks	91
Create Multiple Schedules for a Task	91
Manage Task Schedules	93
UI overview	95
Summary Dashboard	100
Individualize your UI themes	101
Create a custom view	102
Create a custom view from an existing page	109
Change a custom view	110
Change custom views display properties	110
Manage Nerdio Manager Copilot	112
Enable Nerdio Manager Copilot	113
Use Nerdio Manager Copilot	115
Manage Nerdio Manager Copilot's chat settings	117

Submit feedback	118
Disable Nerdio Manager Copilot	118
Build scripts with Nerdio Manager Copilot	120
Generate KQL queries with Nerdio Manager Copilot AnalyticsPro	122
Cost of Nerdio Manager Copilot	125
Functional considerations	127
Deployment considerations	127
Known limitations	127
Desktop Images	128
Management and Lifecycle Tasks for Imported Desktop Images	128
Typical Desktop Image Lifecycle	128
Endpoint Management Software Integration	130
Import Images from the Azure Library	131
Import Custom Azure Managed Images	136
Import an Existing VM	137
Desktop Images Set as Image	140
Desktop Images Scripted Actions	144
Desktop Images Manually Uninstall AVD Agent	146
Use Azure to Backup and Restore Desktop Image VM Objects	147
Create a Desktop Image VM Object Backup Policy	147
Manually Backup a Desktop Image VM Object	148
Restore a Desktop Image VM Object from Azure	149
Clone Desktop Images	150
Desktop Images Change Log Feature	154

Refresh Desktop Images from the Azure Marketplace	156
Stage Desktop Images	157
Enable Desktop Image Staging	157
Edit Desktop Image Staging Auto-activation Settings	159
Deploy an Inactive Staged Desktop Image	159
FSLogix and User Profile Management	161
FSLogix settings and configuration	162
Create an FSLogix profiles storage configuration	162
Set an FSLogix profiles storage configuration as default	165
FSLogix Per-Host Pool Customization	166
FSLogix Shrink VHD/VHDX Containers (Scripted Action)	171
Scripted Actions Overview	173
Create a New Scripted Action	174
View and Edit Existing Scripted Actions	177
Clone a Scripted Action	178
Scripted Actions Groups	178
Apply Scripted Actions	178
Scripted Actions Groups	181
Default Scripts for Nerdio Manager	182
Considerations for Scripted Actions	184
Considerations for Window Scripted Actions	184
Considerations for Azure Scripted Actions	184
Scripted Actions: Azure runbooks variables integration	187
Scripted Actions Global Secure Variables	189

Troubleshoot Scripts	190
Azure Runbooks Logs	190
Troubleshoot Azure Runbooks	191
Troubleshoot Windows Scripts	192
Upgrade Azure Az PowerShell Module	193
Scripted Actions for Windows Scripts	194
Custom Script Extensions	194
Scripted Actions for Azure Runbooks	197
Renew the Azure Runbook Scripted Actions Automation Certificate	199
Scripted Actions for Windows 365	200
Host Pools	204
Workspace Management	205
Create a Workspace	205
Manage Workspaces	206
Create Static Host Pools Without Auto-Scaling	206
Convert a Static Host Pool to Dynamic	211
Add a New Session Host to a Static Host Pool	212
Create Dynamic Host Pools	214
Enable Dynamic Host Pool Auto-scaling	219
Enable Personal Host Pool Auto-scaling	233
Auto-scale: Cost Optimization Session Host VM OS Disk Storage	251
Auto-scale History for Dynamic Host Pools	254
Auto-scale Session Host Scale In-Out Restrictions	257
Add a New Session Host to a Dynamic Host Pool	258

Host Pool Disaster Recovery	260
Host Pool Backup	263
Clone host pools and host pool settings	265
Clone host pools	265
Clone host pool settings	266
Bulk Host Actions	267
Resize/Re-image a Host Pool	270
Restart a Host Pool	273
Power On a Host Pool	274
Power Off a Host Pool	274
Exclude Session Host VMs from Auto-scale During Power On/Off	276
Host Pool AVD Configuration	277
Host pool VM deployment	280
Run Bulk Host Scripted Actions	287
Manage Host Pool User Assignments	289
Apply Host Changes Without Re-Imaging	291
Configure the Host Pool's Active Directory Settings	292
Start VM on Connect for Pooled Host Pools	293
Configure User Session Time Limits	294
Publish Remote Applications to Users	297
Add App Groups to Host Pools	297
Publish RemoteApps to Users	298
Accelerated Networking on Session Host VMs	300
Security	302

Azure Permissions and Nerdio Manager	302
Installation Permissions	302
Subscription Permissions	304
Configuration Permissions	305
Ongoing Use Permissions	307
Role-based Access Control (RBAC) in Nerdio Manager	307
Companion Video	308
Users and Roles Management	308
Add Users to Roles/Workspaces	308
Edit a User's Roles/Workspaces	310
Remove User Access	310
Role-based Access Control (RBAC): Custom Roles	310
Manage user sessions	315
New UI: Manage user sessions	317
Reset FSLogix user profile	318
Windows 365	320
Windows 365: Enable and configure Cloud PCs	320
Enable Windows 365 in Nerdio Manager	320
Hide or display individual Cloud PC hosts page	322
Configure a Windows 365 network connection	324
Manage Windows 365 network connections	325
Create a provisioning policy	326
Edit a provisioning policy	327
Assign licenses to users	327

Access assigned Cloud PCs	328
Manage Cloud PCs	328
Windows 365: Use and Configure Desktop Images for Cloud PCs	329
Create a Desktop Image for Cloud PC	330
Manage Desktop Image for Cloud PC	331
Windows 365: User Settings Policies	334
MSIX App Attach	338
Create and Manage MSIX App Attach Images and Host Pool Assignments	338
Sample VHD(X) Packages and Certificate	338
Upload an MSIX App Attach Image File	339
Upload an MSIX Package File	341
Assign an App to a Host Pool	341
Assign an App Attach v2 App to Users and Groups	342
Use the App Attach v2 Package Wizard	343
Create a New Version of an App	344
Change to a New Version of an App	345
Upload a New Image Version of an App	346
Storage	347
Create and manage configured Azure Files shares	347
Link to an existing Azure Files file share	347
Create a new Azure Files file share and/or storage account	348
Manage configured Azure Files file shares	352
Enable support for Entra ID-joined hosts	353
Auto-scale for Azure Files Storage Premium	355

Auto-scale History for Azure Files Shares	358
Create and Manage Configured Azure NetApp Files	360
Auto-scale for Azure NetApp Files	362
Auto-scale History for Azure NetApp Shares	366
Logs Module	368
Access the Logs Module	368
Configure Logs Retention Policy	369
AI-Powered Personally Identifiable Information Detector	370
Download Application Insights Exceptions Log	370
Gather Application Insights Logs	371

Copyright

Copyright © 2025 by Nerdio, Inc. All Rights Reserved.

The “original instructions” of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Nerdio, Inc. makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Nerdio, Inc. is not obligated to update or correct any information contained in this document. Nerdio, Inc. reserves the right to change products or specifications at any time without notice.

No part of this document may be reproduced in any form for any purpose without the prior written permission of Nerdio, Inc.

The Nerdio, Inc. logo and all Nerdio, Inc. product and service names listed herein are either registered trademarks or trademarks of Nerdio, Inc., or its subsidiaries. All other marks are the property of their respective owners.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

Introduction

Welcome to the Nerdio Manager for Enterprise NME-200 exam curriculum. This curriculum is intended to give you a comprehensive understanding of Nerdio Manager, Microsoft Azure Virtual Desktops, and their various available functions. This curriculum emphasizes the "how to."

The test focuses on the technical configuration and tasks you can, and will, need to execute when deploying, managing, and optimizing your AVD and Windows 365 cloud desktop environments. The test is intended to challenge your retention of critical concepts, features, and methods you will need to successfully work with Nerdio Manager, Azure Virtual Desktops and Windows 365 Cloud PCs.

We highly recommend that you pay close attention when reviewing the curriculum. There are many critical details that will appear in the exam. Simply skimming through the material will most likely be reflected in the outcome of your exam. In addition to the knowledge shared in the curriculum, we expect our test takers to be hands-on Nerdio Manager users. Experience using Nerdio Manager will be invaluable to pass the exam.

Best of luck!

Note: We assume you have the latest version of Nerdio Manager. Some features may not be available in certain versions, so please consult the [Help Center](#) for details.

About Nerdio Manager

Nerdio Manager for Enterprise is a deployment, management, and auto-scaling platform for Azure Virtual Desktop (AVD) and Windows 365 Cloud PC.

Tip: Nerdio Manager for Enterprise is commonly referred to as Nerdio Manager or NME.

Nerdio Manager allows IT professionals and system integrators to deploy, manage, and auto-scale large AVD and Windows 365 Cloud PC desktop environments in the Enterprise. Nerdio Manager can be connected to an existing environment or used to configure a new deployment.

You can operationalize large AVD and Cloud PC deployments through a powerful and intuitive UI used by engineering and help desk staff to deploy the environment and provide on-going user management. Capabilities such as desktop image management, performance monitoring, and user session control eliminate the need for complex scripting and speed up response to end-users.

Nerdio Manager reduces Azure costs with scheduled and event-driven auto-scaling and speeds deployment with a guided setup wizard reducing the engineering workload. Azure compute and storage costs can be reduced by up to 75% and deployment time from weeks to hours. Additional savings result from consolidating user management and monitoring tools and eliminating third-party apps.

And with Nerdio Manager you can reinforce existing security policies, compliance, and address data residency concerns. Nerdio Manager for Enterprise is deployed as an all-PaaS, secure Azure application inside the customer's own subscription in a geographic location of their choice. No user data ever leaves the Azure environment and there is no third-party access to the deployment.



Nerdio Manager is Veracode verified

Directory and identity management

To design, build, and maintain an AVD and Cloud PC environment using Nerdio Manager, it is important to have a good understanding of directory and identity concepts. It is important to understand concepts such as Azure AD, AD Domain Services (on-prem), and Azure AD DS.

In general, Active Directory is a complex topic. Microsoft's multiple directory solutions and deployment models with extremely similar sounding names only make matters even more confusing.

Entra ID - definition of terms

Active Directory Domain Services (Windows Server / on-premises)

- Standard Active Directory role on a traditional Windows server machine that is managed with tools like Active Directory users and computers, sites and services, domains, and trusts.
- Contains user, group, contact, and computer objects.
- Traditional Windows desktops and servers join this AD.
- Users and Groups can be synchronized with Entra ID using Entra ID Connect.

Entra ID - Microsoft Cloud Directory Services

- Despite its similar name to traditional Active Directory, this is a different service that is hosted by Microsoft and is the top-level object in the Microsoft Cloud (O365, D365, and Azure).
- Contains user, group, and contact objects.
- Windows 10 and 11 computers can join Entra ID, while older operating system machines cannot.
- Can be synchronized with a traditional AD via the ADConnect tool, so the same username and password can be used for both (with password hash synchronization enabled).

Entra Domain Services

- An Azure-hosted, Microsoft-managed AD DS.
- Most of the same capabilities as traditional, on-premises AD DS with some limitations due to the lack of administrative access to the actual domain controller, which Microsoft manages.
- Automatically synchronizes with Entra ID, which may be synchronized with on an on-premises AD DS, and allows VMs running in Azure to join it regardless of the type of Windows OS (for example, Windows 11/10/8/7 or Server 2008/2012/2016/2019).

Customers With a Cloud-Only Environment

Entra ID is required to use any of the Microsoft Cloud services (Office 365, Azure Virtual Desktop (AVD), Dynamics 365, etc.). When users access these cloud services, all user authentication begins in Entra ID.

For organizations with “cloud native” deployments, the user information (for example, username, password, group membership, etc.) only resides in Entra ID and is not synchronized with any other directory. If the customer does not have on-premises, line-of-business (LOB) application servers and is not looking to implement virtual desktops in Azure, this Entra ID-only scenario may be sufficient and fairly simple.

Customers With Existing Servers and Applications and/or Virtual Desktops

Most customers start out with existing LOB applications running on-premises and want to migrate these workloads to Azure, reinstall them on new VMs running in Azure, or implement virtual desktops in Azure with AVD. Prior to winter of 2021, AAD alone was not sufficient as LOB servers and virtual desktop VMs must join an Entra Domain Services domain to function and be manageable. Microsoft now supports Entra ID Joined for AVD session hosts, with support for Entra ID Joined for Azure files expected soon (as of November 2021).

Enable Active Directory Functionality in Azure

The following methods are available to enable AD functionality in Azure:

- Do-it-yourself AD in Azure.
- Entra Domain Services PaaS.

Do-it-yourself AD in Azure

Conceptually, the easiest way to create an Azure deployment is:

- Connect to the on-premises network with a site-to-site VPN.
- Deploy a new VM in Azure.
- Join it to the existing AD domain via the VPN.
- Promote it to a domain controller and configure the proper sites/subnets/etc.

What you end up with is an AD deployment that spans both the on-premises network and the Azure deployment with the ability to move server VMs from on-premises to Azure without having to rejoin them to a new domain and without disrupting users' connectivity to these VMs.

The challenge with this deployment lies in the difficulty of implementation, the need to manage new domain controllers, and the cost of additional VMs to run these domain controllers. The advantage is the easy-to-understand deployment for anyone who has managed Active Directory before and complete flexibility with full administrative access.

Azure Active Directory Domain Services (AAD DS) PaaS

To address the challenges with the do-it-yourself AD in Azure method, Microsoft introduced Entra Domain Services--not to be confused with Entra ID.

Entra Domain Services is a PaaS offering in Azure that is operated, monitored, and updated by Microsoft with administrators having limited access. The advantage of Entra Domain Services is that it does not require VMs to be deployed and managed and it does not rely on a VPN to synchronize with an on-premises domain.

When Entra Domain Services is deployed in an Azure subscription, Microsoft creates a pair of high-availability domain controllers and synchronizes the user data from Entra ID.

Entra Domain Services is a new domain that contains read-only copies of users, groups, and password hashes that reside in Entra ID. It synchronizes this data at 20-minute intervals. Azure VMs can be joined to this new domain and existing usernames and passwords can be used to

connect to these VMs since the user credentials are synchronized with Entra ID, which may be synchronized with an on-premises AD using Entra ID Connect.

See this Microsoft [article](#) for more information about Entra ID Connect.

Important:

- Microsoft deploys and manages an Active Directory for you, so you don't have administrative access to it but can connect to manage it with traditional AD management tools (for example, Active Directory Users and Computers or Group Policy Management).
- Entra Domain Services is a new domain that has your existing domain's user objects, if synced using Entra ID Connect.
- User objects that are synchronized from Entra ID to this new domain are read-only. They can only be modified in the source AD (if Entra ID Connect is in use) or Entra ID (if the customer is cloud-only).
- When you create VMs in Azure, they join this new domain. They are not part of your existing domain that is on-premises, only the new domain that is in Azure.
- Servers that are joined to your existing on-premises domain are not part of the new Entra Domain Services domain--only user objects are replicated. There is no trust enabling authentication between the Entra Domain Services and on-premises AD DS environments.
- When doing a lift-and-shift migration of a server from on-premises to Azure with Entra Domain Services enabled, you need to join the server to the new domain and then existing users can be entitled to access it. This requires making changes to the server.
- You need a "management VM" running in Azure with RSAT installed to manage your new Entra Domain Services domain.
- Active Directory Federation Services (AD_FS) functionality, which enables single sign in Office 365, is not supported.
- Directory Schema extensions are not supported.
- There is no way to fail-over the Entra Domain Services domain to another Azure region in case of a regional outage.
- Once deployed, there is no way to pause Entra Domain Services to save on costs without deleting the deployment.

Configure Entra Domain Services for use with AVD

This section applies when you have one of the following situations:

- You have a cloud-only environment. That is, you only have Entra ID and you do not have an on-premises Active Directory with Azure AD Connect.
- You do not want to connect your on-premises domain to the Azure cloud via a VPN.

If any of the above applies, then the Entra Domain Services service provides the Active Directory component required by the Azure Virtual Desktop.

Preliminary Considerations

Important: When you use Entra Domain Services with cloud-only environments, all your AVD users are required to reset their passwords before they can use AVD. This is because the password hashes must be regenerated to be compatible with ADDS (traditional AD). This is one time only after Entra Domain Services has been provisioned. See the [Microsoft documentation](#) for details.

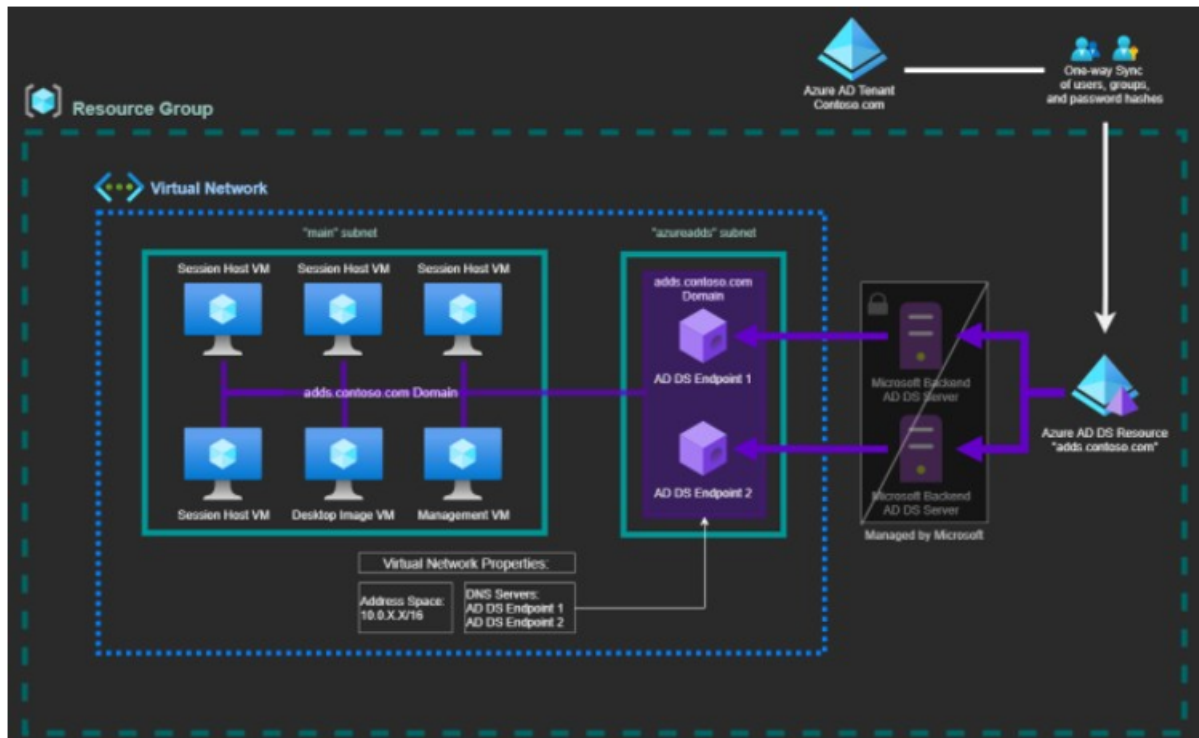
- Entra Domain Services' lowest tier is "standard." **This tier's retail cost is a fixed rate of ~\$110/month** (As of January 2021, prices may vary.) Generally, this tier covers most environments that are under 25,000 AD objects and 3,000 auth/hour. More pricing details can be found [here](#).
- **You do not have Domain Admin rights over the AD.** However, you are given all the necessary management rights to join machines to a domain, edit GPOs and OUs, etc.
- **Entra Domain Services is a one-way sync.** Changes made directly to the AD are not synchronized back up to your Entra ID. Likewise, changes such as adding users, GPOs, OUs, etc. are persistent. However, **if the Entra Domain Services is deleted, the changes are lost.**
- If there are domain-level changes that must be made, such as adding GPOs or OUs, a "Management VM" must be created with RSAT installed to edit the AD. See this [Microsoft article](#) for more information.

- **Entra Domain Services cannot be moved to another resource group or subscription.** It must be deleted and recreated. Keep this in mind if you are using a temporary RG or subscription for PoC purposes.
- **The domain name cannot be changed.** If you are building a PoC and wish to use a temporary domain name, you must delete and recreate the domain.

Entra Domain Services Design Principals

Entra Domain Services is a way to provide domain services such as LDAP, Kerberos/NTLM, domain join, and group policy to various other Azure resources that require them. It takes your cloud-only Entra ID and presents it as if it were a "traditional" or "on-premises" Active Directory to VMs and apps in Azure. It can be thought of as "Active Directory-as-a-service."

This is a sample configuration of Entra Domain Services.



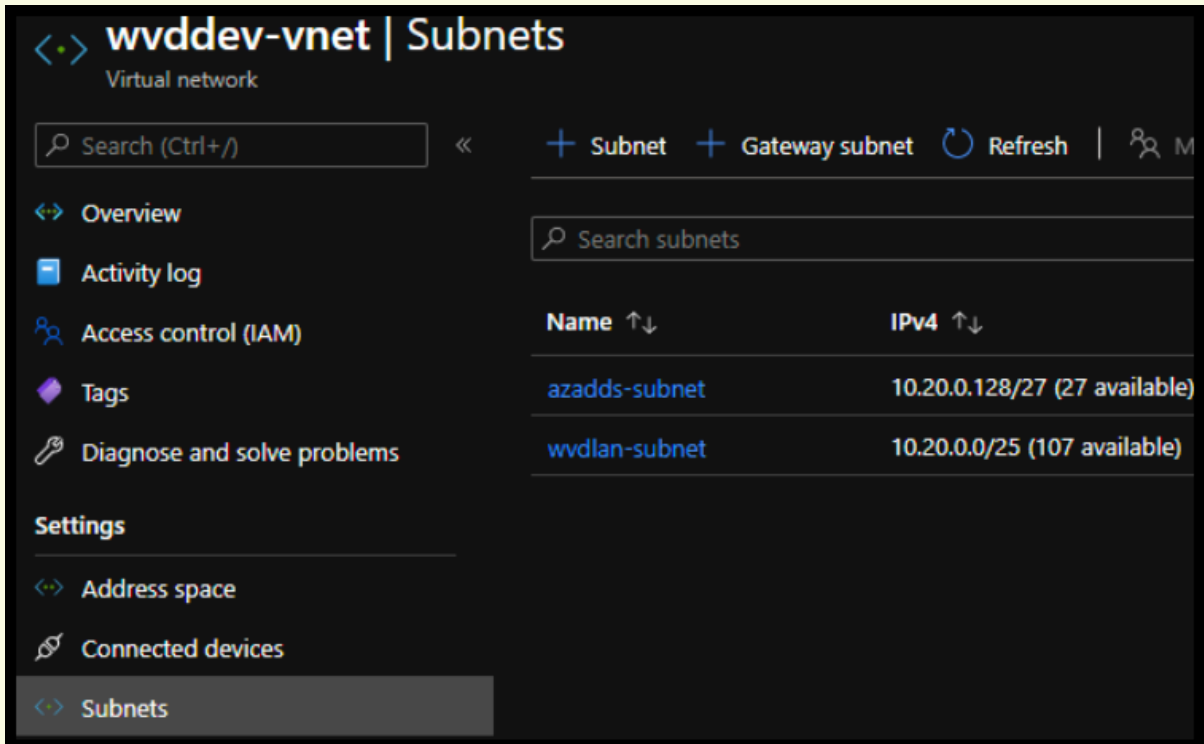
Notes:

- The subnet that Entra Domain Services uses for its endpoints must be separate from your other subnets. It must contain only Entra Domain Services endpoints. Do not attempt to add VMs to this subnet. In addition, it is recommended that you do not link this subnet to your Nerdio Manager environment in the **Settings** section.
- You must set the DNS settings on your virtual network to point to the AD DS endpoints, so that your VMs can resolve the domain.
- Entra Domain Services is a resource object. It can be placed in a resource group and likewise deleted. It is recommended that you set a "lock" to prevent accidental deletion of this resource.

Create an Entra Domain Services Domain

It is recommended that you follow the [Microsoft Guide](#) when creating the environment:

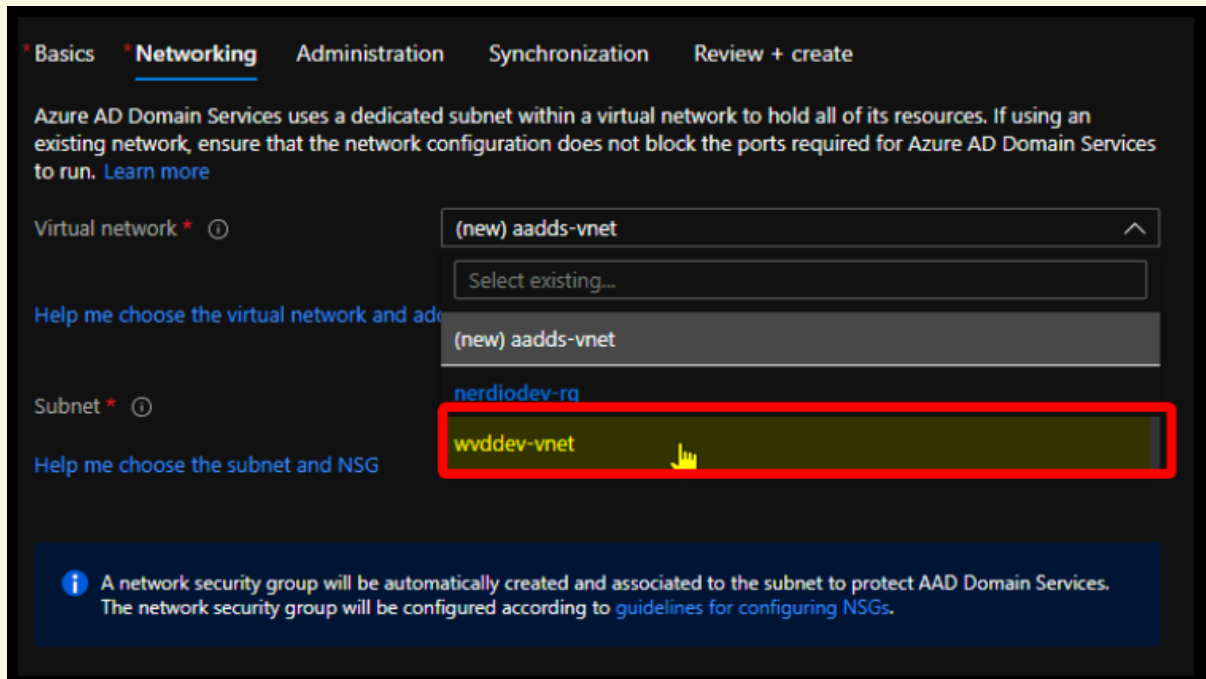
Tip: You need a separate subnet to use for your session hosts. For better organization, before you create your Entra Domain Services, you can make the VNet with two subnets as shown in this example (substitute the IP ranges and names as desired):



The screenshot shows the Azure portal interface for a virtual network named 'wvddev-vnet'. The 'Subnets' tab is active, displaying a table of subnets. The table has two columns: 'Name' and 'IPv4'. The subnets listed are 'azadds-subnet' with an IPv4 range of 10.20.0.128/27 (27 available) and 'wvdlan-subnet' with an IPv4 range of 10.20.0.0/25 (107 available). The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The top navigation bar includes a search bar, a back arrow, and buttons for '+ Subnet', '+ Gateway subnet', 'Refresh', and a search icon.

Name	IPv4
azadds-subnet	10.20.0.128/27 (27 available)
wvdlan-subnet	10.20.0.0/25 (107 available)

In the **Networking** tab, specify the VNet and Subnet you previously created.



Configure Nerdio Manager for Entra Domain Services

When Entra Domain Services is up and running, Nerdio Manager must be configured to utilize it.

To configure Nerdio Manager for Entra Domain Services:

1. Navigate to the **Settings > Azure environment**.
2. Make sure that the **Display non-AD synched users** option is set to **Enabled**.



Note: This allows you to assign users that are cloud-only within Nerdio. Without this setting, users do not appear within the system's web portal for assignments or roles.

Related Topics

[Entra Domain Services Pricing](#)

[Tutorial: Enable User Accounts for Entra Domain Services](#)

[Tutorial: Join a Windows Server VM to an Entra Domain Services Managed Domain](#)

Installation and Getting Started

This section contains topics that help you install and get started using Nerdio Manager.

Nerdio Manager Installation Guide

This section guides you through the process of installing Nerdio Manager in your Azure subscription and initializing Nerdio Manager.

By following these steps, you are registering an Enterprise Application in your own Azure tenant, in a subscription that you select, and into a new resource group. Once the install is complete, you gain access to a URL and are able to sign in to the Nerdio Manager web application.

Nerdio Manager is installed and billed through the Azure Marketplace.

The installation process can be broken down into the following phases:

- Confirm you meet the prerequisites before you start installing Nerdio Manager.
- Install the Nerdio Manager application from the Azure Marketplace listing.
- Initialize the installation by running an Azure PowerShell script.
- Register your installation with our licensing servers and configure the Nerdio Manager settings.

Companion Video

Prerequisites

Note: Sign in to your Azure portal as a Global Administrator, or Privileged Role Administrator and Cloud Application Administrator, before starting the install process.

- You must be a subscription owner of an Azure subscription where you need to install the Nerdio Manager from the Azure Marketplace.

- The Azure subscription must be able to deploy Azure SQL, App Service, Key Vault, Application Insights, and Automation Account in the Azure region you select during the install process.
- You should have a virtual network and a subnet available to deploy AVD session host VMs. You are prompted to select this virtual network and subnet during the configuration phase.
- The custom default DNS server setting specified on the virtual network subnet must point to an AD-aware DNS server or an Azure DNS zone.
- If using Windows Active Directory, Active Directory must be synchronized with Entra ID.
- You need an Active Directory user account with rights to join and unjoin VMs from the domain. This user account must be able to create computer objects in at least one OU in the AD domain and be able to disable these computer objects.
- You need an SMB file storage location for FSLogix Profile containers. This SMB share can be on a file server VM, Azure Files, Azure NetApp Files, or any other location accessible via a UNC path (for example, \\server.domain.local\share\profiles). The server name must be in FQDN format.
 - When using a file share, it must be located in Azure in the same region as the AVD session host's VMs.
 - If you don't have a file storage location available, this step can be skipped during installation, and Nerdio Manager can create Azure Files or NetApp Files after the installation.
- The Microsoft Desktop Virtualization resource provider must be registered in your Azure subscription.

Install Nerdio Manager from the Azure Marketplace

Nerdio Manager is installed from the Azure Marketplace.

To install Nerdio Manager:

1. In the Azure Marketplace, search for Nerdio Manager for Enterprise.
2. Select **Create** > **NME Plan** to start the installation process.

3. Enter the following information:

- **Subscription:** From the drop-down list, select the subscription where you want to install Nerdio Manager.
- **Resource Group:** Select **Create new** to create a new resource group.
- **Region:** From the drop-down list, select the region closest to you or where the majority of your administrators are located.

Note: This region is where the Nerdio Manager web application is located, and does not determine the location of the AVD hosts.

4. Once you have entered all the desired information, select **Next: Review + create**.

5. Review your selections and select **Create**.

Note: A confirmation window displays informing you that the deployment is in progress. The deployment usually takes about 10 minutes.

6. When the deployment is complete, select **Go to resource group**.

7. Locate and select the **App service**.

8. Select **Browse** or select the URL to navigate to your installation of Nerdio Manager.


Initialize Nerdio Manager

When Nerdio Manager for Enterprise is deployed to your Azure subscription, the following steps must be performed to initialize your installation of Nerdio Manager.

Note: If you wish to use Entra ID app registration or Split Identity, skip to "To initialize Nerdio Manager (Entra ID app registration or Split Identity):" on page 31.

To initialize Nerdio Manager (Typical):

1. Sign in to the Nerdio Manager web application as the **Global Administrator**, or **Privileged Role Administrator** combined with **Cloud Application Administrator**, and the subscription **Owner**.
2. Select the copy button to copy the command.



PowerShell

```
& ([ScriptBlock]::Create((Invoke-RestMethod 'https://nwp-web-app.azurewebsites.net/api/package/2.10.0/script/install/cloudshell' -Method POST -Body '{"SubscriptionId":"592e6917-e0f8-4386-a5aa-236b95399cae","ResourceGroupName":"NMW0514","WebAppName":"nmw-app-djjr177x7lhki"}' -ContentType 'application/json').script))
```

Show full script

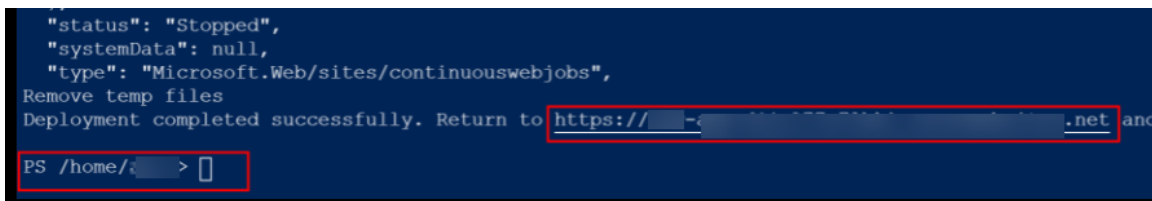
3. Select **Launch Azure Cloud Shell**.



4. If required, select **PowerShell** (not Bash) and create a storage account for the shell history.
5. Paste the PowerShell command and press **Enter**.

Note: Several commands flash by. The script should take about 10 minutes to run.

6. When the script completes, you are returned to the prompt. The message **Deployment completed successfully** is displayed.



```
"status": "Stopped",
"systemData": null,
"type": "Microsoft.Web/sites/continuouswebjobs",
Remove temp files
Deployment completed successfully. Return to https://... .net and
PS /home/... > 
```

7. Select the URL in the confirmation message. Alternatively, return to the open tab in the browser and refresh the page. You are now ready for the next phase of the installation process - "Configure Nerdio Manager Settings" on the next page.

To initialize Nerdio Manager (Entra ID app registration or Split Identity):

1. Sign in to the Nerdio Manager web application as the **Global Administrator**, or **Privileged Role Administrator** combined with **Cloud Application Administrator**, and the subscription **Owner**.
2. Select **Show advanced**.
3. For Entra ID app registration:
 - **Use existing Entra ID app registration**: Select this option.
 - **App ID**: Type the App ID.
 - **App Secret**: Type the App secret.
 - **Service Principal ID**: Type the service principal ID.
4. For Split Identity:
 - **Split Identity**: Select this option.
 - **Identity Tenant ID**: Type the identity tenant ID.
5. Select **Download script (Az)**.
6. From your local machine, locate and run the downloaded script.
7. Select the URL in the confirmation message. Alternatively, return to the open tab in the browser and refresh the page. You are now ready for the next phase of the installation process.

Configure Nerdio Manager Settings

Nerdio Manager is now installed. The next step is to configure various application settings.

When you navigate to the URL, you see a window similar to this:

Welcome to Nerdio Manager for Enterprise

You have successfully installed Nerdio Manager in your subscription!

Now let's connect Nerdio Manager to your Azure environment. You will be able to start creating and managing Azure Virtual Desktop resources once the configuration is done. Follow the checklist below to complete the configuration.

Nerdio Manager Configuration

- Feature set**
Select your desired feature set. Select between 'AVD' and 'Intune' modes.
 - AVD
 - Intune & Windows 365
- Entra ID Tenant**
Tenant: Nerdio University
ID: [REDACTED]
- Azure subscription**
Name: Microsoft Azure
ID: [REDACTED] (AVD, Deployment, VMs)
- Nerdio Manager registration**
Status: Unregistered. [Click to register](#)
- Network**
Select virtual network with access to Active Directory and FSLogix file share.
vNet: [none selected](#)
- Resource Group**
Select Resource Group that will contain AVD session host VMs.
Name: [ETC-Demo-NME-RG](#)
- Directory**
Connect to an existing Active Directory, Entra Domain Services or native Entra ID.
Name: [none selected](#)
- File storage**
Select a location where FSLogix profile containers will be stored, or create a new Azure Files share
Location: [none selected](#)
- Windows 365 & Intune integration**
Enable if you would like to manage Windows 365 & Intune devices. Intune integration for Unified Endpoint Management allows enrolled Windows devices to be reported on and managed directly in the Nerdio Manager console. Please review the requirements below before proceeding.
Current status: [Disabled](#)
- User cost attribution**
Report on per-individual-user costs based on allocation of the total cost of AVD deployment (compute, storage, network, PaaS, SaaS) to individuals based on duration of their usage of AVD desktops during the selected time frame.
[Enable](#)

You already provided some settings in the previous steps. Those settings are checked off, which indicates they are completed. The settings that need your attention are unchecked. As you complete a setting, the system automatically checks off that setting.

Note: You do not have to provide the settings all at once. You can safely return to this page at any point. Your settings are retained and you won't need to enter the settings again. This page is displayed every time you return to the URL of the app service until all the steps have been completed.

To configure the Nerdio Manager settings:

1. In the **Feature set** section, select your desired feature set:

- AVD
- Intune & Windows 365

Note: You can set up AVD only or both feature sets at the same time.

2. In the **Nerdio Manager registration** section:

- Select **Click to register**.
- Enter your registration information.
- Once you have entered all your registration information, select **Register**.

3. In the **Network** section:

- Select **none selected**.
- **Subnet:** From the drop-down list, select the subnet.
- Select **OK**.

4. In the **Resource Group** section:

Tip: By default, the same resource group contains both the Nerdio Manager resources (for example, app services) and the AVD session host VMs. It is recommended that you create a new resource group in the Azure portal and use it for the AVD session host VMs.

- Select the resource group name.
- **Resource Group:** From the drop-down list, select the destination resource group.
- Select **OK**.

5. In the **Directory** section:

Note: The Active Directory, Entra Domain Services, or native Entra ID user account must have permission to create computer objects in the domain. Nerdio Manager uses these credentials when joining computers to the domain.

In addition, when using Active Directory, the user account needs some extra permissions to join Azure Files shares to the directory.

- Select **none selected**.
- Enter your Active Directory, Entra Domain Services, or native Entra ID information.
- Once you have entered all the desired information, select **OK**.

6. In the **File storage** section:

Note: You can provide your FSLogix file storage information or a UNC path to an existing file share accessible from the VNet. If you don't have a file share ready, select the option to skip this step.

- Select **none selected**.
- **Skip this step for now:** Select this option to skip this step and configure the file storage later.
- **FSLogix:** Select the FSLogix version. Default is the latest version.
- **Use Cloud Cache:** Select this option to enable FSLogix Cloud Cache in the host pools, and the session hosts within those host pools, that use this FSLogix profile.

Tip: For performance reasons, it is strongly recommended that you use Premium SSD and Ephemeral OS disks when Cloud Cache is enabled. Standard SSD disks might be sufficient in very small environments or for testing scenarios.

Note: See the following Microsoft [document](#) for more information about FSLogix Cloud Cache.

Cloud Cache allows you to specify multiple profile storage locations. It asynchronously replicates the profiles and makes the profiles available in multiple storage locations at the same time. So, if one of the locations is not available, the session host automatically fails over to one of the alternate locations.

- **Configure session hosts registry for Entra ID joined storage:** Select this option to enable Entra ID Kerberos functionality and Entra ID account credentials loading.

Note: For more information, see [Configure the session hosts | Microsoft Learn](#).

- **FSLogix Profiles path:** From the drop-down list, select an Azure Files share or Azure NetApp Files volumes. Alternatively, type in a UNC path.

Note: You can specify up to 4 paths. In addition, use the arrows to change the order of the paths. The profiles are created in all of these locations.

- Once you have entered all the desired information, select **OK**.
7. Optionally, in the **Windows 365 & Intune integration** section:
 - Select **Disabled**.
 - Review the prerequisites.
 - Enable the required configuration features.
 - Select **OK**.
 8. Next to **User cost attribution**, select **Enable**.

Note: For details on enabling Windows 365 in Nerdio Manager, see [Windows 365 - Enable and Configure Cloud PCs](#).

To complete the installation process:

1. Once you have configured all the settings noted above, select **Done**.
2. Select the link of the tenant that is provided.
3. Sign in, review, and then accept the consent.
4. Navigate back to Nerdio Manager and select **I have granted admin consent**.
5. Select **OK**.

Note: If there are any errors, please repeat the consent steps. It sometimes takes several minutes. You can retry it a few times until the consents are validated.

The installation is now complete, and you are ready to start using Nerdio Manager.

Nerdio Manager Edition Management

Nerdio Manager has two editions-- **Core** and **Premium**. The Nerdio Manager Premium edition has all the features found in the Core edition, plus many others.

Please see our [website](#) for details about the features and pricing.

Warning: Downgrading from Premium to Core could result in loss of functionality. For example, advanced cost optimization features are not supported in the Core edition. Therefore, if a customer downgrades to Core, and they were making use of features such as Azure Capacity Extender, these features are no longer available

Nerdio Manager allows you to change your edition at any time.

To change your edition of Nerdio Manager:

1. Navigate to **Settings > Nerdio environment**.
2. In the **Product edition** tile, select the Product edition name.
3. Review the confirmation pop-up.

Tip: When downgrading to Core, the confirmation pop-up displays a detailed list of the functionality you lose access to. Be sure to review it carefully before proceeding.

4. When you are ready to change your edition, select **OK**.

Your edition of Nerdio Manager is changed.

Note: Prior to version 6.0 of Nerdio Manager, customers could purchase either the Standard or Premium editions of the product. The licensing options described above only apply to new Nerdio Manager installations for version 6.0 and later.

Update the Nerdio Manager application

Nerdio releases regular updates for Nerdio Manager, but Nerdio Manager does not automatically update itself. Instead, it gives version control to the administrators. There are several methods that can be used to update Nerdio Manager to the latest version. Due to possible restrictions in some environments, alternative methods may be required.

Nerdio Manager updates FAQs

Will updating Nerdio Manager interrupt currently active sessions or kick off users?

No. The update process only affects the Nerdio Manager App Service. User sessions are handled by the AVD service, which is managed and hosted separately by Microsoft. The only interruptions that occur affect the Nerdio management console. In addition, the auto-scale automation is unable to perform actions during the update process. Auto-scale automation safely continues automatically after the update process is completed.

How long does the update process take?

Using the Automation Account, the process generally takes ~3-7 minutes, as all actions are performed in Azure. When done manually, using the standalone installer through PowerShell, this time is affected by local variables such as the internet connection and client machine's hardware. The data files are roughly 120-160MB in size.

It may take several minutes for Nerdio Manager to complete processing background updates and the portal to be available again after the update has been successfully applied.

Can I skip over versions when updating?

Yes. All updates are cumulative, and it is **recommended** that you skip intermediate versions and go directly to the latest Generally Available release. For example, you can update directly from 2.2.0 to 2.10.1.

Can I rollback to a previous version?

Starting with version 6.3, you can rollback to a previous version, but you can only rollback to 6.2 or later. For example, 6.4 can be rolled back to 6.3 or 6.2, but not earlier. See "Restore Nerdio Manager to a previous version" on page 46 for details.

Method 1: Deploy button

The simplest method for updating Nerdio Manager is to use the **Deploy** button.

Note: This process must be completed by a user with Contributor or Automation Operator rights to the Azure Automation account deployed by Nerdio Manager.

To update using the deploy button:

1. In Nerdio Manager, navigate to **Updates**.
2. Locate the latest version and select **Deploy**.
3. Monitor the Azure automation job, under the **Output** tab, and watch until the **Status** is reported as **Completed**.

Method 2: Use Azure Cloud Shell (v2.10+)

You may use Azure Cloud Shell to update Nerdio Manager.

Note: This process must be completed by a user with the Contributor rights to the Nerdio Manager App Service.

To update using Azure Cloud Shell:

1. In Nerdio Manager, navigate to **Updates**.
2. Locate the latest version and from the action menu select **Azure Cloud Shell**.

DEPLOY VERSION 3.5.0


Copy the command below. Then click to launch Azure Cloud Shell, paste the copied command and press ENTER. Be sure that you're logged into Azure as a user with **Contributor** access to the Nerdio Manager App Service.

```
& ([ScriptBlock]::Create('$sourceUri = "https://nwmstorageaccount.blob.core.windows.net/nwm-';
```

[Show full script](#)

Launch Azure Cloud Shell

Once the script completes running, return to this page and refresh it.

3. Select the copy script icon  to copy the script to the clipboard.
4. Select **Launch Azure Cloud Shell**.

5. In Azure Cloud Shell, paste the script and press **Enter**.
6. When the script run is completed, refresh the **Updates** page.

Method 3: Standalone PowerShell update

You may use PowerShell to update Nerdio Manager.

Note: This process must be completed by a user with the Contributor rights to Nerdio Manager's deployment resource group.

To update using PowerShell:

1. In Nerdio Manager, navigate to **Updates**.
2. Locate the latest version and from the action menu, select **Download Installer**.
The installer is downloaded as a .zip file to your browser's default download folder.
3. Right-click the downloaded .zip file and select **Properties**.
4. At the bottom of the **General** tab, select **Unblock** and then select **OK**.
5. Extract the .zip file to a location on the C: drive.
6. Open PowerShell.
7. Change the directory to the folder with the extracted installer.
8. Run **DeployUpdate.ps1** and follow the instructions.
9. When the installation is completed, refresh the **Updates** page.

Method 4: Manual "Zip Push" deployment

You may use the "Zip Push" method in the Azure portal to update Nerdio Manager.

Prior to redeploying the new package, you need to clear the existing application from the App Service. You can do this using the Kudu service portal or the Advanced Tools Console.

Note: This process must be completed by a user with the Contributor rights to the Nerdio Manager App Service.

To update Nerdio Manager using the "Zip Push" method:

1. In Nerdio Manager, navigate to **Updates**.
2. Locate the latest version, and then from the action menu, select **Download Installer**.

The installer is downloaded as a .zip file to your browser's default download folder. Ensure you save this package to a safe location.

3. Expand the package file and retrieve the file named **site.zip** or **app.zip**. Only one file is included.

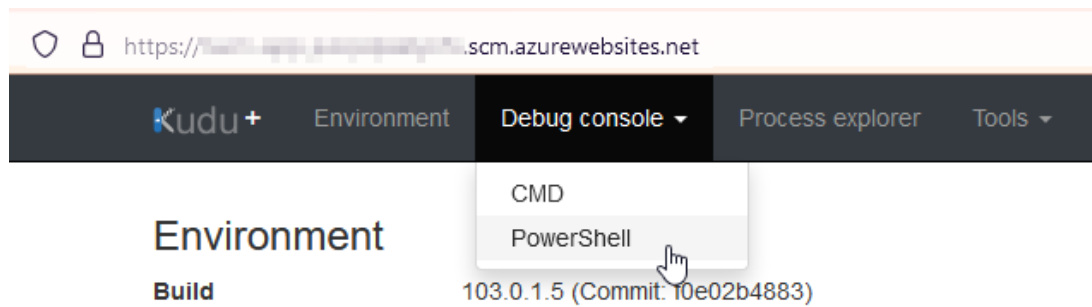
Warning: Do not unzip or expand the **site.zip** or **app.zip** file.

4. In the [Azure portal](#), navigate to **App Services > Nerdio Manager App Service**.

Note: The Nerdio Manager App Service name is typically prefixed with **nmw-app**. Make sure you don't confuse it with the App Service named **nmw-cc1-app**, which is used for Cost Attribution.

5. In the left menu, navigate to **Development Tools > Advanced Tools**, and then select **Go** to launch the Kudu console.
6. Clear the existing application from the App Service:

- a. In the top toolbar, select **Debug Console > PowerShell**.



- b. Change **location** to the **site\wwwroot** directory. Use one of the following paths:

- **cd C:\home\site\wwwroot**
- **Set-Location C:\home\site\wwwroot**

- c. Run one of the following commands to clear all files from the directory:

- **del *.***
- **Remove-Item *.***

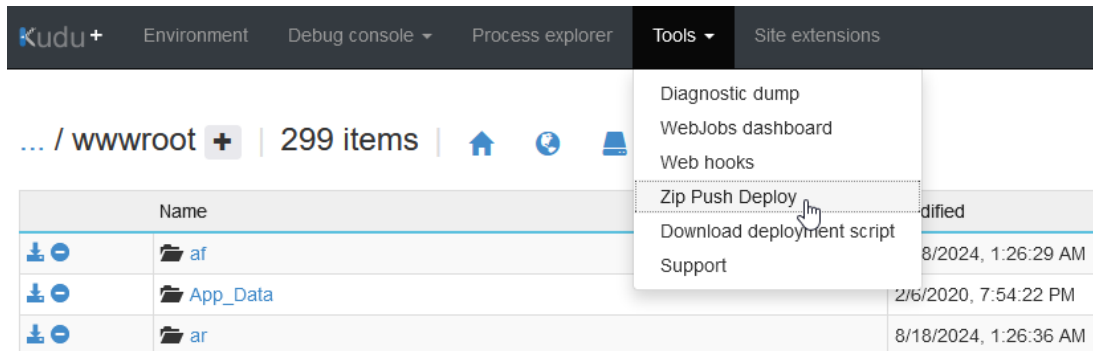
Note: The folders can remain in the directory.

```
Kudu Remote Execution Console
Type 'exit' then hit 'enter' to get a new powershell process.
Type 'cls' to clear the console

PS C:\home> Set-Location C:\home\site\wwwroot
Set-Location C:\home\site\wwwroot
PS C:\home\site\wwwroot> Remove-Item *.*
```

7. Redeploy the app package:

- a. In the Kudu console toolbar, go to **Tools > Zip Push Deploy**.



- b. In the file explorer dialog box, drag the **site.zip** or **app.zip** file that you retrieved from the package file you previously downloaded.

Warning:

- Make sure you drag only the **site.zip** or **app.zip** file, rather than the **package.standalone*.zip**, which prevents Nerdio Manager from running successfully.
- Ensure the file's extension is **.zip**.

The lower section of the page updates to reflect the package uploading and deploying. Wait until the final task displays **Deployment successful**.

8. Run the **provision** WebJob:
 - a. In the Azure portal, navigate to **App Service > Settings > WebJobs**.
 - b. Select the **provision** job and make sure that its status is **Running**. If it's **Stopped**, in the **Run** column, select the play button, and then select **Start**.

Note: If the WebJob named **provision** is missing, the wrong zip file was uploaded to Nerdio Manager's App Service. Verify and re-upload the **site.zip** file only (do not upload the full **package.standalone*.zip** file).

9. Return to the Nerdio Manager app and refresh your browser to confirm the app is online and accessible.

Method 5: Manual Azure Cloud Shell deployment

You can use Azure Cloud Shell to update Nerdio Manager.

Note: This process must be completed by a user with the Contributor rights to Nerdio Manager App Service.

To update Nerdio Manager using Azure Cloud Shell:

1. Open [Azure Cloud Shell](#).
2. Customize and run the script below.
3. When the script finishes running, return to the Nerdio Manager app and refresh the browser page to confirm the app is online and accessible.

```
$sourceUri = "Obtain URL from Nerdio support (nme.support@getnerdio.com)"
$subscriptionId = "Your Subscription ID containing the NMW app service"
$resourceGroupName = "Resource Group name that contains NMW app service"
$webAppName = "WebApp Name (e.g. nmw- app- xxxxxxxxxxxx, not including
azurewebsites.net)"
$version = "App version to update to (e.g. 6.4.1)"
$webjobName = "Provision"
Set-PSDebug -Strict
$ErrorActionPreference = "stop"
Write-Output "Downloading package"
$folderName = (New-Guid).ToString()
$packageZipPath = Join-Path -Path $Home -ChildPath ($folderName + ".zip")
$packageDestPath = Join-Path -Path $Home -ChildPath ($folderName)
$packageDestVersionPath = Join-Path -Path $packageDestPath -ChildPath "version.txt"
$packageDestAppPath = Join-Path -Path $packageDestPath -ChildPath "app.zip"
Write-Output "Destination: $packageZipPath"
Invoke-WebRequest -Uri $sourceUri -OutFile $packageZipPath
Expand-Archive -Path $packageZipPath -DestinationPath $packageDestPath
az account set -s $subscriptionId
az configure --defaults group=$resourceGroupName web=$webAppName
Write-Output "Stop web job"
az webapp webjob continuous stop --webjob-name $webjobName
Start-Sleep -Seconds 10
```

```
Write-Output "Stop web app"
az webapp stop
Start-Sleep -Seconds 10
Write-Output "Deploy package"
az webapp deploy --src-path $packageDestAppPath --clean
Start-Sleep -Seconds 10
Write-Output "Start web app"
az webapp start
Start-Sleep -Seconds 10
Write-Output "Start web job"
az webapp webjob continuous start --webjob-name $webjobName
Start-Sleep -Seconds 10
Write-Output "Remove temp files"
Remove-Item -Path $packageZipPath
Remove-Item -Path $packageDestPath -Recurse
Write- Output "Version $version completed successfully. Return to
https://$webAppName.azurewebsites.net and refresh the browser page."
```

Restore Nerdio Manager to a previous version

Starting with version 6.3, you can restore a previous version, but you can only downgrade to 6.2 or later. For example, 6.4 can be downgraded to 6.3 or 6.2, but not earlier.

To restore to a previous version:

1. In Nerdio Manager, navigate to **Updates**.
2. Locate the version you want to downgrade to and select **Deploy**.

3. Under the **Output** tab, monitor the Azure automation job and watch until the **Status** is reported as **Completed**.

Note: When restoring from version 6.7 to an earlier version, there is a known issue where all dashboard values are reported as 0 (zero) if the option to include all costs is configured. To prevent this issue, from the user cost attribution dashboard (**Dashboard > User cost attribution**), delete any configurations with the **include all costs** option selected before you start the redeployment.

Nerdio Manager Default Deployment Resources and Costs

When you install the Nerdio Manager application from the Azure Marketplace, the following resources are automatically created.

- Automation Account
- SQL Server and SQL Database (S1)
- Application Insights
- App Service Plan and App Service (B3)
- Key Vault

The initial deployment is sized to accommodate thousands of AVD users. The SQL Database and App Service have some Azure costs associated with them.

- App Service (B3) - \$219/month (list price)
- SQL Database (S1) - \$29/month (list price)

For small-scale pilot deployments, you can scale down the App Service as low as B1 (\$55/month) and SQL Database as small as B (\$5/month). This can be done live in the Azure portal without shutting down the application. However, keep in mind that this may have an impact on how responsive Nerdio Manager might be with such small resource sizes.

For large deployments (10,000+ AVD users), you can increase the size of the SQL Database and App Service.

Setup and Settings

This section contains topics that help you set up Nerdio Manager.

Harden Nerdio Manager

By restricting network traffic, Nerdio Manager can be hardened in the following areas:

- **Storage Accounts:** These are used by both AVD and Nerdio Manager to store various sorts of data. Most notably, storage accounts are used for holding end-user's FSLogix Profiles, boot diagnostics, custom scripted actions, and MSIX app attach packages.
- **SQL:** Nerdio Manager relies on communication between two Azure PaaS services: Azure App Service and Azure SQL Database. By default, this communication is encrypted with Transport Layer Security, and data at rest is also encrypted using Transparent Data Encryption.
- **App Service:** The entry point into the Nerdio Manager application is the App Service. By default, the Nerdio Manager App Service is protected with Entra ID authentication, including MFA and conditional access, and is accessible from any internet location.
- **Key Vaults:** Key Vaults allow for the secure storage and access of secrets. These include API keys, passwords, and certificates. SQL connectivity is also dependent on the key vault due to this being the storage location for the SQL connection string.

Note: This topic discusses hardening Nerdio Manager using a script. You may manually harden Nerdio Manager components. For details, see the following topics:

- "Harden Azure Storage Account" on page 54
- "Harden SQL" on page 59
- "Harden App Service" on page 51

An Azure runbooks script is available to add private endpoints and service endpoints to allow the Nerdio Manager app service to communicate with the SQL database and the Azure Key Vault over a private network, with no traffic routed over the public internet. Access to the SQL database and the Azure Key Vault is restricted to the private network.

Note: When enabling private endpoints, if the storage account that stores scripted actions is made private, then Azure runbooks scripted actions stop working. The fix for this is to use the Hybrid Worker option with scripted actions. The Hybrid Worker VM needs to be on a VNet that has access to the storage account. If using the private endpoint script, that means the Hybrid Worker VM needs to be on the peered VNet or the private endpoints VNet that the private endpoint script creates.

Requirements

- The App Service Plan, which is essentially the "performance tier" for the server that is hosting the app, must support VNet integration. Please see this Microsoft [article](#) for details on supported plans.
- A virtual network (VNet) that can be used to connect to the App Service and the Storage Account. This virtual network needs outbound access for Nerdio Manager to talk to Nerdio licensing servers via HTTPS (TCP/443).

Warning: Variables specified in clear text are visible in the Azure Automation logs. To pass sensitive data use Global Secure Variables. See "Scripted Actions Global Secure Variables" on page 189 for details.

To harden Nerdio Manager:

1. Navigate to **Scripted Actions > Azure runbooks**.
2. Find the script **Enable Private Endpoints**.
3. From the action menu, select either **Run now** or **Schedule**.
4. Enter the following optional values:

- **PeerVnetId:** Optionally, type the Resource ID for an existing network.

Note: This is the Resource ID of the VNet to peer to the private endpoint VNet. Supplying a Resource ID for an existing network causes that network to be peered to the new private network. Nerdio recommends against peering to other production networks in hardened scenarios, unless (1) access to storage account has been restricted, or (2) the app service has been configured as private.

- **StorageAccountResource:** Optionally, type the storage account to be included in private endpoint subnet.

Note: Access to this storage account is restricted to Nerdio Manager and peered VNets. This parameter only accepts a single storage account, which should be an Azure Files location.

- **MakeAppServicePrivate:** Set to **true** to limit access to the Nerdio Manager application.

Note: If set to true, only hosts on the VNet created by this script, or on peered VNets, are able to access the app service URL.

5. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).



Nerdio Manager is Veracode verified

Harden App Service

Nerdio Manager consists of a number of PaaS services. The entry point into the Nerdio Manager application is the App Service. By default, the Nerdio Manager app service is protected with Entra ID authentication, including MFA and conditional access, and is accessible from any internet location. It is possible to further protect the Nerdio Manager app service by using Access Restrictions or enabling a Private Endpoint.

Note: Azure app services also have FTP services enabled by default. These can be fully disabled for Nerdio Manager.

Requirements

To use VNet integration, in some instances, the App service plan must be **Standard**, **Premium**, **PremiumV2**, or **PremiumV3**. Please note that some **Basic** plans support Vnet integration. See this Microsoft [article](#) for details. In addition, see Upgrade the Azure App Service for upgrade options.

Configure Access restrictions on the Nerdio Manager App Service

1. In the Azure portal, locate the Nerdio Manager App Service resource.

Note: It typically has a name in the following format: **nmw-app-xxxxxxxxx**.

2. Within the menu on the left-hand side of the App Service blade, scroll down to the **Settings** section.
3. Select **Networking**.

Note: By default, the configuration is to allow all access.

4. In the **Inbound Traffic** section, select **Access restriction**.
5. Select **+Add**.

6. Type the **Name** and **Description** of the new rule.
7. Ensure that **Action** is set to **Allow**.
8. Specify the source IP address block to allow access.

Note: This automatically adds a new "Deny All" rule to the list to prevent access from all other locations.

9. Select **Add rule**.
10. Once all rules have been applied, navigate to **App Services** > [your Nerdio Manager App Service name] > **Settings** > **Networking** > **Public Network Access Restrictions**.
11. Under **Site access and rules**, on the **Advanced tool site** tab, select the **Use main site rules** option.

Access Restrictions ⋮

Save Refresh

App access

Public access is applied to both main site and advanced tool site. Deny public network access will block all incoming traffic except that comes from private endpoints.

Public network access ⓘ

Enabled from all networks (This will clear all current access restrictions)
 Enabled from select virtual networks and IP addresses
 Disabled

Site access and rules

Main site Advanced tool site

You can define lists of allow/deny rules to control traffic to your site. Rules are evaluated in priority order. If no created rule is matched to the traffic, the "Unmatched rule action" will control how the traffic is handled. [Learn more](#) ⓘ

Unmatched rule action

Allow
 Deny

Use main site rules ⓘ

+ Add 🗑 Delete

Action : All
×

Priority ↑ ▾	Name ▾	Source ▾	Action ▾	HTTP headers ▾
2147483647	Allow all	Any	✔ Allow	Not configured

After a few minutes, only allowed IP ranges are able to connect to the Nerdio Manager application.

Create a Private Endpoint on the Nerdio Manager App Service

1. In the Azure portal, locate the Nerdio Manager App Service resource.

Note: It typically has a name in the following format: **nmw-app-xxxxxxxx**.

2. Within the menu on the left-hand side of the App Service blade, scroll down to the **Settings** section.
3. Select **Networking**.
4. In the **Inbound Traffic** section, select **Add**.
5. Type a custom **Name** for the private endpoint.
6. Choose the **Subscription** containing your VNet.
7. Select the **VNet** and **Subnet** where the private endpoint should be attached.
8. Optionally, depending on your VNet DNS configuration, you may be able to select the option for **Integrate with private DNS zone**.

Notes:

- Most customers specify custom DNS servers targeting their internal AD environment, in which case this option may be disabled.
- If **Integrate with private DNS zone** is not enabled, be sure that the DNS is properly configured to resolve your private endpoint. See [Azure Private Endpoint DNS Configuration](#) for details.

9. Select **OK** to save the private endpoint.

After a few minutes, any connections to Nerdio Manager's app service routing to the public IP addresses is rejected. Only connections that resolve your Nerdio Manager URL to the private endpoint IP address succeed.

Disable FTP Services on the Nerdio Manager App Service

1. In the Azure portal, locate the Nerdio Manager App Service resource.

Note: It typically has a name in the following format: `nmw-app-xxxxxxxx`.

2. Within the menu on the left-hand side of the App Service blade, scroll down to the **Settings** section.
3. Select **Configuration**.
4. Navigate to the **General settings** tab.
5. On the **FTP state** selector, change the option from **All allowed** (default) to **Disabled**.
6. Select **Save**.

FTP services are now disabled for Nerdio Manager's app service.

Related Topics

"Harden Nerdio Manager" on page 48

"Harden Azure Storage Account" below

"Harden SQL" on page 59

Harden Azure Storage Account

Storage Accounts are used by both AVD and Nerdio Manager to store various sorts of data. Most notably, storage accounts are used for holding end user's FSLogix Profiles, boot diagnostics, custom scripted actions, and MSIX app attach packages. This topic covers key steps and important considerations when implementing tighter security for common scenarios using storage accounts.

Requirements

- The App Service Plan (essentially the "performance tier" for the server that is hosting the App) needs to be upgraded from the default of Basic (B3), to Standard or Premium. This means increased operating costs. See Upgrade the Azure App Service for details.

- A virtual network (VNet) that can be used to connect the App Service and the Storage Account. This virtual network also needs outbound access for Nerdio Manager to talk to the Nerdio licensing servers via HTTPS (TCP/443). The licensing server URL is <https://nwp-web-app.azurewebsites.net/>.

Warning: Without VNet integration, Nerdio Manager is unable to connect to a storage account with network restrictions enabled. See this Microsoft [article](#) for more information.

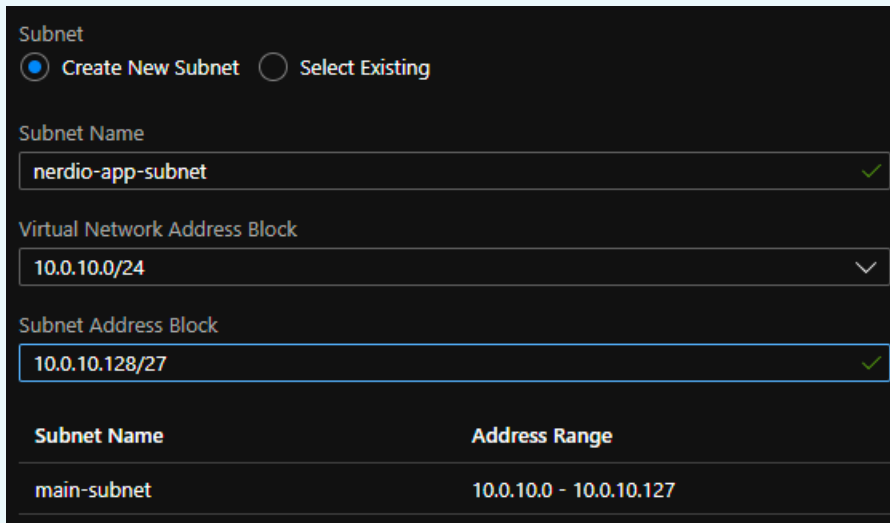
Enable VNet Integration for Nerdio Manager's App Service

1. In the Azure portal, locate the Nerdio Manager App Service resource.

Note: It typically has a name in the following format: `nwm-app-xxxxxxxx`.

2. Within the menu on the left-hand side of the App Service blade, scroll down to the **Settings** section.
3. Select **Networking**.
4. In **VNet Integration**, select **Click here to configure**.
5. In **VNet Configuration**, select **Add VNet**.
6. Select the VNet you wish to use.
7. Select **OK**.

Note: VNet integration requires a subnet delegated specifically for use with app services. This cannot be shared with any other Azure resources. The subnet selected for integration needs to be /28 or larger. It may be necessary to add an additional subnet that is compatible for the integration if there are no unused subnets or subnets not delegated for other services. In this example, there was already a VNet used for session hosts, which still had unallocated IP address ranges within the address block, so a new subnet was created specifically for the app service VNet integration.



Subnet Name	Address Range
main-subnet	10.0.10.0 - 10.0.10.127

When the VNet is successfully integrated, the page should look something like this:

VNet Configuration

Securely access resources available in or through your Azure VNet. [Learn more](#)

VNet Details

VNet NAME	wvd-vnet
LOCATION	West US 2

VNet Address Space

Start Address	End Address
10.0.10.0	10.0.10.255

Subnet Details

Subnet NAME	nerdio-app-subnet
-------------	-------------------

Subnet Address Space

Start Address	End Address
10.0.10.128	10.0.10.159

Harden the Storage Account

Warning: Incorrectly implementing this restriction can cause session hosts to lose access to FSLogix profiles, user data, MSIX apps, software data, etc. Be sure to take these new network restrictions into consideration before proceeding.

1. In the Azure portal, navigate **Storage accounts**.
2. Locate and select the storage account you wish to harden.
3. Within the menu on the left-hand side of the Storage accounts blade, scroll down to the **Security + networking** section.
4. Select **Networking**.

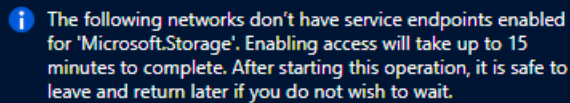
5. In the **Firewalls and virtual networks** tab, enter the following:

- **Allow access from:** Select **Selected networks**.
- Select **+ Add existing virtual network**.
- **Virtual networks:** From the drop-down list, select the VNet(s) and Subnets you wish to use.

Note: If the storage account contains user profiles, be sure to link all subnet(s) containing AVD session hosts, to ensure FSLogix can mount the user profiles successfully.

- Select **Enable**.

Note: If you receive a message like this, that means it will take time for the changes to fully take effect. This is normal and expected.



i The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait.

6. Once you have entered all the desired information, select **Save**.

7. In Nerdio Manager, refresh the console and check the storage account locations. Alternatively, attempt to perform an action that previously led to an error due to improper storage account restrictions, such as linking an MSIX App Attach storage location or enabling storage auto-scaling.

Related Topics

"Harden Nerdio Manager" on page 48

"Harden App Service" on page 51

"Harden SQL" on the next page

Harden SQL

Nerdio Manager relies on communication between two Azure PaaS services: Azure App Service and Azure SQL Database. By default, this communication is encrypted with Transport Layer Security, and data at rest is also encrypted using Transparent Data Encryption.

In order to further protect communication between the App Service instance and the SQL database, it is possible to restrict network traffic in two different ways, as detailed in this article.

- **Add the App Service's Outbound IP addresses to the Azure SQL Server's firewall.** This method ensures that only requests from your Nerdio Manager instance's IPs are able to reach the server. However, the Azure App Service is hosted on shared infrastructure. Any other App Services deployed to the same cluster as Nerdio Manager shares the same outbound IPs.

Note: IP addresses associated with the app service cluster may change or update over time. It may be required to periodically update the firewall with any changes to cluster IP addresses. We recommend using VNet and Subnet whitelisting to avoid this inconvenience.

- **Route traffic from the App Service using a VNet.** Create an Azure SQL service endpoint in the VNet. Traffic to the SQL Server can then be restricted to allow only traffic coming from the VNet.

Restrict SQL Traffic to App Service Outbound IPs

In order to restrict SQL traffic to the App Service's IP addresses, we first must discover the IPs the app is using.

1. Optionally, run the following PowerShell or CloudShell command:

```
Login-AzAccount  
  
(Get-AzWebApp - ResourceGroup <group_ name> - name <app_  
name>).OutboundIpAddresses
```

This returns several IPs associated with your Nerdio Manager App Service. Outbound requests might come from any of the IPs shown.

2. In Azure portal, search for SQL Servers, and find the **nmw-app-sql-*** server.
3. Within the menu on the left-hand side of the SQL Server blade, scroll down to the **Security** section.
4. Select **Networking**.
5. In the **Public access** tab, enter the following information:
 - Select **Selected networks**. (default option)
 - Enter a rule for each IP address associated with your App Service.
 - Unselect **Allow Azure services and resources to access this server**.
6. Once you have entered all the IPs, select **Save**.

Traffic to the SQL Server is now restricted to these addresses.

Routing App Service Traffic through a VNet

If restricting traffic to your App Service's outbound IPs is not adequate for your security needs, you can route all App Service traffic through a VNet, and restrict SQL traffic to that VNet.

Notes:

- VNet integration requires the App Service to be a Standard plan or higher. See [Upgrade the Azure App Service](#) for details.
- An existing or new VNet may be used for the VNet integration.

Enable VNet Integration for Nerdio Manager's App Service

See "Enable VNet Integration for Nerdio Manager's App Service" on page 55 for details.

Harden the SQL Server

1. In Azure portal, search for SQL Servers, and find the **nmw-app-sql-*** server.
2. Within the menu on the left-hand side of the SQL Server blade, scroll down to the **Security** section.
3. Select **Networking**.
4. In the **Public access** tab, enter the following information:
 - Select **Selected networks**. (default option)
 - Add the desired **Virtual networks** and **Firewall rules**.
 - Unselect **Allow Azure services and resources to access this server**.
5. Once you have entered all the desired information, select **Save**.

Traffic from the Nerdio Manager App Service is now routed through your virtual network to the SQL Server service endpoint. Only traffic from your virtual network is allowed to connect to the database.

Related Topics

"Harden Nerdio Manager" on page 48

"Harden App Service" on page 51

"Harden Azure Storage Account" on page 54

Back up and restore Nerdio Manager configuration

This article discusses how to back up and restore the Nerdio Manager configuration.

Post-February 2025: Updated backup strategy

As of February 2025, we updated our backup and restore strategy. The following sections outline our current recommendations on this topic.

Important: We encourage you to review and follow the updated processes. However, if you've already implemented the legacy backup method, you can continue using it as described in "Pre-February 2025: Legacy backup strategy" on page 68.

Nerdio Manager is an Azure application consisting of several PaaS services. When backing it up, consider the following components:

- **Azure Key Vault:** This contains service principal secrets and AD domain joiner user account passwords. The contents of the Key Vault are fairly static and do not need to be backed up on a regular basis.
- **Azure SQL Database:** This contains auto-scale configuration (for example, scheduling), logs, and auto-scale history data. The relevant contents of the database change when auto-scale settings are modified. A recurring backup is recommended.
- **Azure App Service:** This runs the Nerdio Manager application and does not contain actual data beyond the application binaries. The contents of the app service change when the application is upgraded to the latest version.

Tip: The recommended method for backing up Nerdio Manager is to use the default backups for both the App Service and SQL Server, which are automatically configured by Azure when the resources are created. The process for configuring custom backups is covered below.

Since Azure does not provide a built-in backup process for Key Vaults, a script will be used to back up certificates, keys, and secrets.

For Nerdio Manager configuration components and their built-in restore functionality, see Nerdio Manager SQL Database Restore: Host Pool Matrix.

Prerequisites

Ensure the following prerequisites are met.

Area	Details
Scripts download	Select this link to download the .zip file that contains the scripts used in the steps below. Once you download the zip file, unzip it on your local computer.
Azure	A non-guest account with at least Contributor role permissions on the Key Vault, which can be inherited from the subscription the Key Vault is tied to.
Local	<ul style="list-style-type: none"> • PowerShell 6.2.4 or PowerShell 5.1 for Windows. PowerShell 7.1 for

Area	Details
system	<p>Windows is not supported.</p> <ul style="list-style-type: none"> The entire Azure PowerShell Module "Az", or individual modules "Az.Accounts", "Az.KeyVault", "Az.Resources", "Az.Storage", and "Az.Websites". For details, see How to install Azure PowerShell. .Net Framework 4.7.2 or later.

App Service automatic backups

By default, Azure enables an hourly automatic backup of the App Service.

To view the automatic backups:

1. In the Azure portal, navigate to **App Services > NME App Service**.
2. In the left menu, navigate to **Settings > Backups**.

The hourly automatic backups are displayed on this page.

App Service custom backups

If needed, you can customize Azure automatic backups to use a specific schedule, custom retention settings, and include a linked database.

Note: Databases up to 4 GB can be backed up via the App Service backup. For larger databases, SQL Server-provided backups must be used instead.

For details, see [Back up and restore your app in Azure App Service](#).

To back up the App Service and SQL database:

1. Locate the downloaded `app-service-backup.ps1` script on your local computer.
2. Retrieve the following values:

Value	Steps
Azure subscription ID	Go to Nerdio Manager > Settings > Azure environment > Azure subscriptions tile. Note: Both the App Service and backup storage account should be located in the same Azure subscription.
App Service resource group name	Go to Nerdio Manager > Settings > Azure environment > Linked resource groups tile.
App Service name	Go to Azure portal > Resource groups , and look up the name.
Storage account resource group	Go to Azure portal > Resource groups , and look up the name. Note: This can be the same as the App Service resource group name.
Storage account name	Go to Azure portal > Resource groups , and locate the name.

3. On your local computer, run the **app-service-backup.ps1** script and provide the values as requested.

Note: When prompted to sign in, use an account with permissions to the App Service and storage account. A user with Contributor permissions on the subscription is recommended.

After the script runs, backups of the App Service and SQL database are performed automatically every day, with a retention period of 15 days.

Note: By default, the script sets a retention period of 15 days and runs every day at the same time it was initially executed.

To modify the retention period:

1. In the Azure portal, navigate to **App Service**.
2. Go to **Settings > Backups**, and select **Configure custom backups**.
3. Customize the settings as needed.
4. Ensure the SQL connection string is present before you select **Save**. If the value is missing, you can retrieve it from the **Secrets** tab in the Key Vault provisioned by Nerdio, under the name '**ConnectionStrings-DefaultConnection**'.

Alternatively, you can run the `app-service-backup.ps1` script with the `-retentionPeriodInDays` parameter, specifying the desired retention period.

SQL Server backups

By default, Azure enables a daily automatic backup of the database. For detailed steps, see [Change automated backup settings for Azure SQL Database](#).

To view and modify SQL backups:

1. In the Azure portal, navigate to **SQL servers > NME SQL server**.
2. In the left menu, navigate to **Data management > Backups > Retention policies**.
3. Modify the retention policy to change the backup frequency and retention periods.

Key Vault backup

You can back up the Key Vault using two alternative methods:

- With the **Backup NMW App** scripted action in Nerdio Manager.
- With a PowerShell script that retrieves the certificates, keys, and secrets stored within the Key Vault, and saves them to a local zip file named `keyvault-backup.zip` in the same directory where the script is run. The contents of the zip file are encrypted and can only be decrypted in the original Key Vault region in Azure.

Warning: This process creates a one-time backup. No scheduling is configured. If a recurring backup is required, you can schedule the **Backup NMW App** scripted action from Nerdio Manager.

To back up the Key Vault using a PowerShell script:

1. Locate the downloaded `key-vault-backup.ps1` script on your local computer.
2. Retrieve the following values:
 - **Azure Subscription name:** Go to Nerdio Manager > **Settings** > **Azure environment** > **Azure subscriptions** tile.
 - **Key Vault name:** Go to the Azure portal and look up the name.
3. On your local computer, run the `key-vault-backup.ps1` script and provide the values as requested.

Note: When prompted to sign in, use a non-guest account with Access policies and permissions for the Key Vault. A user with Owner role is recommended.

4. After the script runs, the `keyvault-backup.zip` backup file is present in the directory.

Note: Be sure to save the backup file (`keyvault-backup.zip`) in case you need it for a future restore.

Key Vault restore

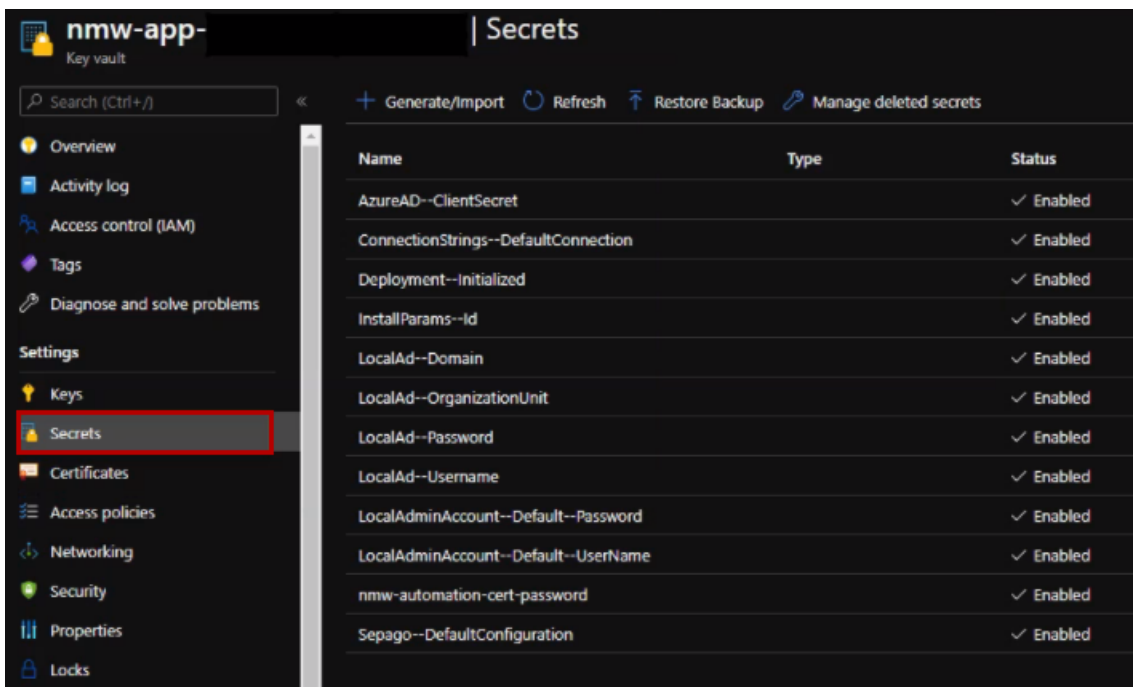
The following procedure restores the Key Vault from a backup.

Note: The backups taken in the previous process only support in-region restores, meaning the restore process fails if the vault's contents are restored to a new region.

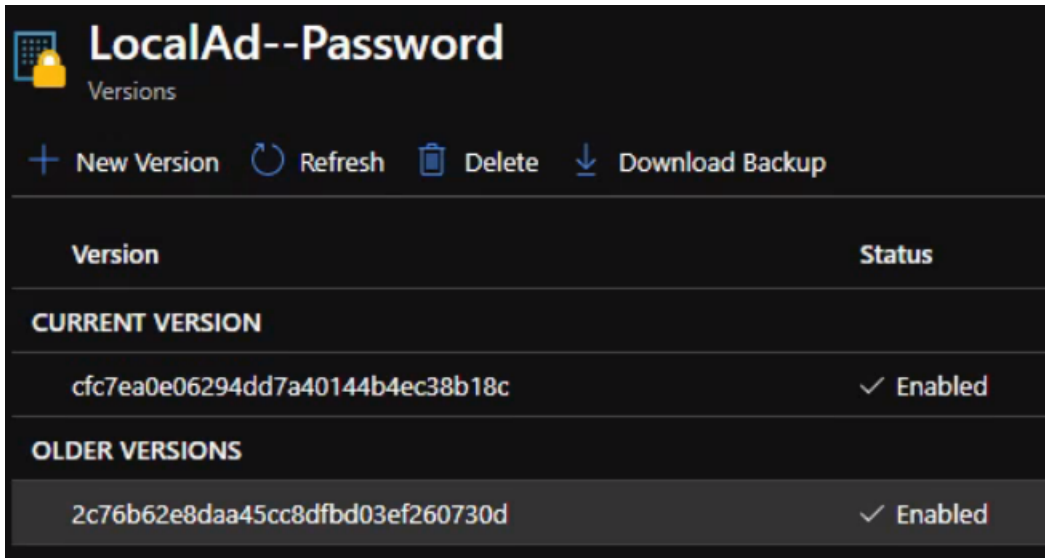
To restore the Key Vault from a backup:

1. Locate the downloaded `key-vault-restore.ps1` script on your local computer.
2. Move the `key-vault-restore.ps1` script to the same directory as the `keyvault-backup.zip` file.
3. Run the `key-vault-restore.ps1` script.

Note: The script restores only keys, secrets, and certificates that do **not** exist. If they have been deleted, but not purged, you receive a conflict error from the script. When restoring to a Key Vault with existing values, those values are not overwritten.



Note: You can manually restore old secrets from the portal by selecting the **Older Versions** of the secret. This is useful if a specific value has been changed and needs to be reverted, such as the password used by the AD account.



Pre-February 2025: Legacy backup strategy

This section covers how to back up and restore the Nerdio Manager configuration using the recommended backup strategy prior to February 2025.

Important: We encourage you to review and follow the updated processes as described in "Post-February 2025: Updated backup strategy" on page 61. However, you can still use the legacy backup method if already implemented.

Nerdio Manager is an Azure application consisting of several PaaS services. When backing up Nerdio Manager, consider the following components:

- **Azure Key Vault:** This contains service principal secrets and AD domain joiner user account passwords. The contents of the Key Vault are fairly static and do not need to be backed up on a regular basis.
- **Azure SQL Database:** This contains auto-scale configuration (for example, scheduling), logs, and auto-scale history data. The relevant contents of the database change when auto-scale settings are modified. A recurring backup is recommended.
- **Azure App Service:** This runs the Nerdio Manager application and does not contain actual data beyond the application binaries. The contents of the app service change when the application is upgraded to the latest version.

Tip: The recommended method for backing up Nerdio Manager is to enable App Service backups and directly retrieve the contents of the Key Vault used by Nerdio Manager to a .zip file. SQL database backups are automatically included with the App Service backups.

For Nerdio Manager configuration components and their built-in restore functionality, see Nerdio Manager SQL Database Restore: Host Pool Matrix.

In this section:

- "Prerequisites" below
- "App Service and SQL DB Backup" on the next page
- "Key Vault backup" on page 72
- "App Service restore" on page 73
- "Key Vault restore" on page 74

Prerequisites

Area	Details
Scripts download	Select this link to download the .zip file that contains the scripts used in the steps below. Once you download the zip file, unzip it on your local computer.
Azure	<ul style="list-style-type: none"> • A non-guest account with at least Contributor role permissions on the Key Vault, which can be inherited from the subscription the Key Vault is tied to. • A storage account used by the app-service-backup.ps1 script needs to be created. • If the SQL Server has been hardened (limiting network access to known VNets and IPs only), all IP addresses associated with the app service cluster must be added as permitted IPs on the SQL Server firewall (associated IP addresses are displayed on the Networking tab of the app service). Otherwise, the backup services for the App Service are

Area	Details
	<p>unable to connect to the SQL server and save the backup successfully.</p> <ul style="list-style-type: none"> App Service backups occur in the app service cluster, and do not use any configured private endpoints or VNet integration.
Local system	<ul style="list-style-type: none"> PowerShell 6.2.4 or PowerShell 5.1 for Windows. <p>Note: The entire Azure PowerShell Module "Az", or individual modules "Az.Accounts", "Az.KeyVault", "Az.Resources", "Az.Storage", and "Az.Websites". For details, see How to install Azure PowerShell.</p> <ul style="list-style-type: none"> .Net Framework 4.7.2 or later.

App Service and SQL DB Backup

The following procedure backs up the App Service and SQL database.

To back up the App Service and SQL database:

1. Locate the downloaded `app-service-backup.ps1` script on your local computer.
2. Retrieve the following values:

Value	Steps
Azure subscription ID	<p>Go to Nerdio Manager > Settings > Azure environment > Azure subscriptions tile.</p> <p>Note: Both the App Service and backup storage account should be located in the same Azure subscription.</p>
App Service resource group name	<p>Go to Nerdio Manager > Settings > Azure environment > Linked resource groups tile.</p>
App Service name	<p>Go to Azure portal > Resource groups, and look up the name.</p>

Value	Steps
Storage account resource group	Go to Azure portal > Resource groups , and look up the name. Note: This can be the same as the App Service resource group name.
Storage account name	Go to Azure portal > Resource groups , and locate the name.

3. On your local computer, run the **app-service-backup.ps1** script and provide the values as requested.

Note: When prompted to sign in, provide an account with permissions to the App Service and storage account. A user with Contributor permissions on the subscription is recommended.

4. After the script runs, backups of the App Service and SQL database are performed automatically every day, with a retention period of 15 days.

Note: By default, the script sets a retention period of 10 days and runs every day at the same time it was initially executed.

To modify the retention period:

1. In the Azure portal, navigate to **App Service**.
2. Go to **Settings > Backups**, and select **Configure custom backups**.
3. Customize the settings as needed.
4. Ensure the SQL connection string is present before you select **Save**. If the value is missing, you can retrieve it from the **Secrets** tab in the Key Vault provisioned by Nerdio, under the name '**ConnectionStrings-DefaultConnection**'.

nmw-app- | Backups ☆ ...

Backup Now **Configure custom backups** Reset custom backups Restore Refresh Troubleshoot Documentation

App backups happen automatically every hour. If you need a different backup schedule, you can also configure custom backups, but you'll also need to set up a separate storage account. To start the restore process, select a backup. Automatic backups retention schedule follows different patterns. [Learn more](#)

Oldest backup: 12/12/2024 Automatic backup: Every 1 hour

Type: All Status: All Time range: None Add filter Reset

Showing 10 of 248 results

Backup time	Status	Type	Restore
10/03/2025, 10:02:50	Succeeded	Automatic	Restore
10/03/2025, 09:02:50	Succeeded	Automatic	Restore
10/03/2025, 08:02:50	Succeeded	Automatic	Restore
10/03/2025, 07:02:49	Succeeded	Automatic	Restore
10/03/2025, 06:02:49	Succeeded	Automatic	Restore
10/03/2025, 05:02:49	Succeeded	Automatic	Restore
10/03/2025, 04:02:48	Succeeded	Automatic	Restore

Backup Storage

Select the target container to store your app backup.

Storage Settings nmw-backups Storage Account: tblob.core.windows.net

Backup Schedule

Configure the schedule for your app backup.

Scheduled backup: On Off

Backup Every * 1 Days Hours

Start backup schedule from * 10/15/2020 1:42:12 PM (UTC-08:00) Pacific Time (US & Canada)

Retention (Days) * 10

Keep at least one backup: No Yes

Key Vault backup

You can back up the Key Vault using a PowerShell script that retrieves the secrets and certificates stored in the Key Vault, and saves them to a local zip file named **keyvault-backup.zip** in the same directory where the script is run. The contents of the zip file are encrypted and can only be decrypted in the original Key Vault region in Azure.

Warning: This process creates a one-time backup. No scheduling is configured. If a recurring backup is required, you can schedule the **Backup NMW App** scripted action from Nerdio Manager.

To back up the Key Vault:

1. Locate the downloaded **key-vault-backup.ps1** script on your local computer.
2. Retrieve the following values:
 - **Azure subscription name:** Go to Nerdio Manager > **Settings** > **Azure environment** > **Azure subscriptions** tile.
 - **Key Vault name:** Go to the Azure portal and look up the name.
3. On your local computer, run the **key-vault-backup.ps1** script and provide the values as requested.

Note: When prompted to sign in, use a non-guest account with Access policies and permissions for the Key Vault. A user with Owner role is recommended.

4. After the script runs, the **keyvault-backup.zip** backup file is present in the directory.

Note: Be sure to save the backup file (**keyvault-backup.zip**) in case you need it for a future restore.

App Service restore

You can restore the App Service using the portal option within the App Service, or using the files stored in the storage account under the **nmw-backup** blob container.

For details, see:

- [Restore an app in Azure.](#)
- [Restore deleted App Service app Using PowerShell](#)

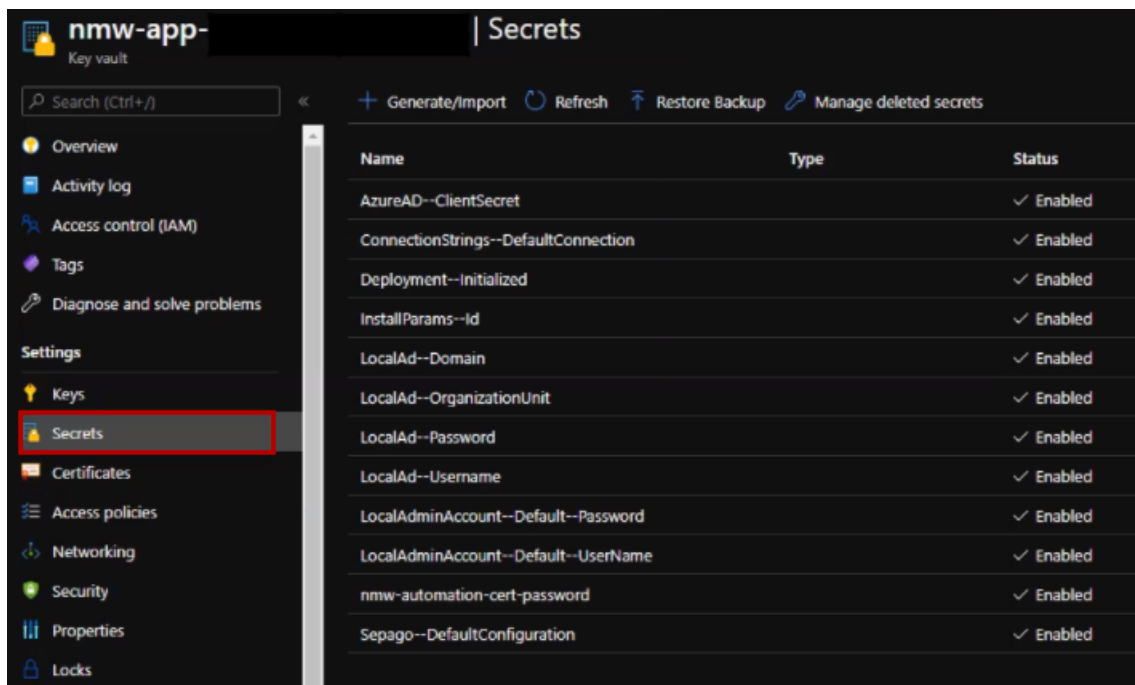
Key Vault restore

The following procedure restores the Key Vault from a backup.

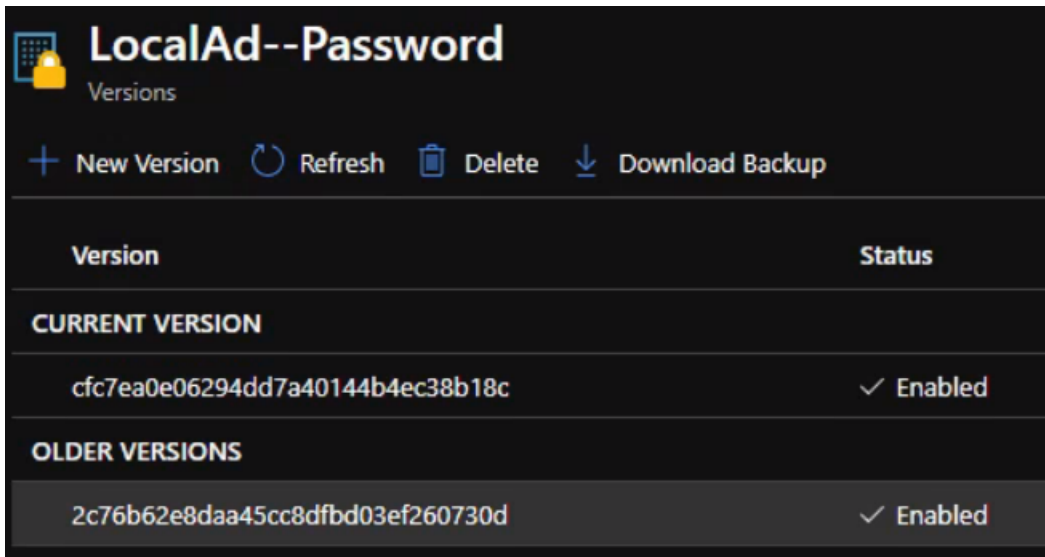
To restore the Key Vault from a backup:

1. Locate the downloaded `key-vault-restore.ps1` script on your local computer.
2. Move the `key-vault-restore.ps1` script to the same directory as the `keyvault-backup.zip` file.
3. Run the `key-vault-restore.ps1` script.

Note: The script restores only secrets and certificates that do **not** exist. If they have been deleted, but not purged, you receive a conflict error from the script. When restoring to a Key Vault with existing values, those values are not overwritten.



Note: You can manually restore old secrets from the portal by selecting the **Older Versions** of the secret. This is useful if a specific value has been changed and needs to be reverted, such as the password used by the AD account.



Alerts and notifications

Nerdio Manager notifications allow you to define rules to generate email alerts based on various conditions and actions, such as failed tasks, auto-scale actions, or role changes. Select whom to notify based on tasks, statuses, resources, etc. Notifications are defined by a condition and a corresponding action or actions to be triggered when the condition occurs.

Note: You must enable email notifications before you start to configure conditions and actions. See Configure Email Notifications for details.

Create a new Intune alert condition

Intune alert conditions allow you to define the parameters that will match this alert condition and therefore trigger a notification action.

To create a new Intune alert condition:

1. Navigate to **Notifications** and select the **Intune Alert Conditions** tab.
2. Select **Add**.
3. Enter the following information:
 - **Name:** Type the name of the condition.
 - **Alert Type:** From the drop-down list, select the type of alert.
 - **Severity:** Select the severity of the alert.
4. Once you have entered the desired information, select **OK**

CREATE INTUNE ALERT CONDITION

Name	<input type="text" value="Intune Alert"/>
Alert Type	<input style="border: 1px solid #ccc; border-radius: 4px; padding: 2px 10px;" type="text" value="Intune configuration policy issues"/> x v
Severity ⓘ	<input checked="" type="radio"/> High <input type="radio"/> Warning

Cloud PC alert conditions

Nerdio Manager provides a number of pre-configured Cloud PC alert conditions that can be activated or edited

To edit a Cloud PC alert notification:

1. Navigate to **Notifications** and select the **Cloud PC Alert Conditions** tab.
2. Select an alert condition, and select **Edit**.
3. Enter the following information:

- **Severity:** Select the severity for the alert condition
- **Enabled:** Toggle this option **On** to enable the alert condition.
- **Portal pop-up:** Toggle this option **On** to enable in-console notifications on the alert condition.
- **Send email:** Toggle this option **On** to and add an email address to receive alert impact, summary, and next steps from the Intune Portal.

4. Select **OK** to save and exit.

To activate a Cloud PC alert notification:

1. Navigate to **Notifications** and select the **Cloud PC Alert Conditions** tab.
2. Select an alert condition, and from the the drop down, select **Activate**.

CLOUD PC ALERT CONDITIONS		
STATUS	NAME ⓘ	SEVERITY ⓘ
●	Azure network connection failure	Warning
●	Cloud PCs are in grace period	Warning

Edit

- Activate

3. Select **OK** in the activate this notification rule dialog box.

Create a new Nerdio Manager alert condition

Nerdio Manager alert conditions allow you to define the parameters that will match this alert condition and therefore trigger a notification action

To create a new Nerdio Manager alert condition:

1. Navigate to **Notifications**, and select the **Nerdio Manager Alert Conditions** tab.
2. Select **Add**.
3. Enter the following information:

- **Name:** Type the name of the condition.

Note: You need to specify this name when creating a corresponding notification action.

- **Targets:** From the drop-down list, select the target(s).

Note: The targets can include all tenants or workspaces, or they can be confined to a specific tenant or workspace, or a single host pool.

- **Tasks:** From the drop-down list, select the task(s).

Note: These are the action or actions that are evaluated. Examples include Add host, Disconnect user session, Stop VM, etc.

- **Run By (User):** From the drop-down list, select the interactive user(s) or background process(es) that triggered the task.
- **Statuses:** From the drop-down list, select the status(es) (for example, completed, error, or canceled) that this condition should match.
- **Exclusion Keywords:** Type the exclusion keyword(s) to be used to suppress notifications that contain these keyword(s).

Note: The keywords help to detect and suppress false positives.

4. Once you have entered the desired information, select **OK**.

The condition is created.

Note: From the Notifications Conditions page, you may edit or delete conditions.

Examples of conditions

Auto-scale errors: This condition triggers when any task started by the Auto-scale User results in an error.

NOTIFICATIONS - UPDATE CONDITION

Define the parameters that will match this condition and trigger a Notification action

NAME: ⓘ

TARGETS: x | v ⓘ

TASKS: x | v ⓘ

RUN BY (USER): x | v ⓘ

STATUSES: x | v ⓘ

EXCLUSION KEYWORDS: | v ⓘ

Role Changes: This condition triggers when any changes are made to user roles.

NOTIFICATIONS - UPDATE CONDITION

Define the parameters that will match this condition and trigger a Notification action

NAME: ⓘ

TARGETS: x | v ⓘ

TASKS: x
 x | v ⓘ
 x

RUN BY (USER): x | v ⓘ

STATUSES: x | v ⓘ

EXCLUSION KEYWORDS: | v ⓘ

Failed Desktop Image Creation: This condition triggers when either the "Power off & set as image" or the "Update 'set as image' schedule configuration" tasks end in an error.

NOTIFICATIONS - UPDATE CONDITION

Define the parameters that will match this condition and trigger a Notification action

NAME: ⓘ

TARGETS: x | v ⓘ

TASKS:
 x | v ⓘ

RUN BY (USER): x | v ⓘ

STATUSES: x | v ⓘ

EXCLUSION KEYWORDS: v ⓘ

Create a new action

Actions are the .notifications to send out if a condition is matched.

To create a new action:

1. Navigate to **Notifications**, and select the **Actions** tab.
2. Select **Add**.
3. Enter the following information:
 - **Nerdio Conditions:** From the drop-down list, select the conditions(s) to match.
 - **Cloud PC Conditions:** From the drop-down list, select the conditions(s) to match.
 - Optionally, select the **Activate disabled Cloud PC alert conditions** to enable disabled Cloud PC alert conditions.

Note: Cloud PC alert notifications are triggered when one or more condition rules are matched. Disabled Cloud PC alert conditions are marked with warning colors and can be enabled by selecting **Activate disabled Cloud PC alert conditions** .

- **Intune Conditions:** From the drop-down list, select the conditions(s) to match.
- **Include task detail:** Select this option to include the task detail in the body of the email and attach it as a JSON file.
- **Send emails on event:** Toggle this option **On** to send emails on event.
 - **Send From:** From the drop-down list, select a linked email address that is used to send the notification.

Note: Only linked mailboxes in are displayed. See Configure Email Notifications for details.

- **Send To:** Type the email address(es) to send the notifications to.

Note: Multiple emails can be specified separated by commas.

- **Trigger webhook on event:** Toggle this option **On** to trigger a webhook on event.

Note: See Configure Microsoft Teams Notifications Using Webhooks for details about configuring webhooks.

- **Webhook:** From the drop-down list, select the webhook to send the notifications to.

4. Once you have entered the desired information, select **OK**.

NOTIFICATIONS - CREATE ACTION

Specify pre-defined conditions, that will trigger an email notification, the source and destination email addresses and/or destination webhook.

NERDIO CONDITIONS: Product update available x v ⓘ

CLOUD PC CONDITIONS: Cloud PCs are in grace period [Disabled] x v ⓘ

Activate disabled Cloud PC alert conditions ⓘ

INTUNE CONDITIONS: Select... v ⓘ

Include task details ⓘ

Send emails on event On

SEND FROM: @getnerdio.com x v ⓘ

SEND TO: @getnerdio.com ⓘ

Trigger webhook on event On

WEBHOOK: NME-Webhook x v ⓘ

Cancel OK

The action is created.

Note: From the Notifications Actions page, you may edit, deactivate, or delete actions.

Configure Azure Monitor Alerts for AVD Resources

Azure Monitor is a comprehensive native monitoring solution that can be utilized to send alerts for given parameters. See this Microsoft [article](#) for details.

Of the many capabilities Azure Monitor possesses, AVD administrators and engineers are most interested in its ability to monitor session host VMs, storage accounts, and other resources used by Nerdio Manager and AVD. While Nerdio Manager does not incorporate alert functionality, it is possible to construct custom Azure monitor alerts to achieve the same desired effect.

The following table shows some examples of Azure monitoring.

Area to Monitor	Azure Signal	Description
Session Host VMs	Data IOPS	<p>This is a common issue with some VM sizes because the VM disk bandwidth is too low, and loading a large FSLogix profile causes long sign in times. By monitoring for this, you can determine if you have under-provisioned the session host VMs.</p>
Storage Account Metrics (FSLogix Profiles and AppAttach)	Used Capacity	<p>You can set a GB size threshold that is near the quota.</p> <p>Note: In most cases the quota is created to an excessively large size as IOPS performance is tied to file share quota size. This alert is not useful for these situations. However for cost-savings or smaller environments, a small quota or standard-tier may be provisioned.</p> <p>For example, set the threshold to 2 GB (make sure to select the correct value under "Unit", default is GB, not GiB). The granularity and frequency of evaluation can be set as desired.</p>
SQL Databases (Nerdio ManagerApp Backend)	DTU Percentage	<p>SQL databases can be monitored as well. For some operations, such as viewing auto-scale history, a large amount of logs may be queried and parsed, causing a large demand for DTUs.</p> <p>SQL tends to be notoriously tricky to evaluate in terms of performance. However, this monitoring should suffice to detect a significant throttling of DTUs which affects Nerdio Manager's functionality, and can manifest itself in errors such as "Execution</p>

Area to Monitor	Azure Signal	Description
		Timeout Expired."
App Service (Nerdio Manager Application)	N/A	See "To create a Service Health Alert" on the next page below.

To create an Alert Rule:

1. In the Azure portal, navigate to **Virtual machines**.
2. Select the VM you wish to work with.
3. On the blade on the left side, in the **Monitoring** section, select **Alerts**.
4. Select **+ Create > Alert rule**.
5. Enter the following information in the following tabs:

- **Scope:** Select the scope.

Note: When creating Alert rules, you can select multiple resources of the same type. For example, you may want to select all VMs in this resource group. Doing so means the alerting does not need to be enabled on each VM individually. This is entirely up to your discretion.

- **Condition:** Select the condition to monitor. See the table above.

Note: After selecting the specific value to be measured, you are then prompted for additional parameters. These settings need to be adjusted depending on your specific situation. See this Microsoft [article](#) for details.

- **Actions:** Select the actions to take. For example, you can create a simple email notification.

Note: If no action groups have been previously created, you can do that now. See this Microsoft [article](#) for details.

- **Details:** Enter the Alert rule name, description, etc.

Note: Severity is up to your preference, as it is used to sort alerts from the Alerts panel. See this Microsoft [article](#) for details.

- **Review + create:** Review the information and select **Create**.

The Alert Rule is created.

To create a Service Health Alert

1. In the Azure portal, navigate to **Service Health**.
2. Select **+ Add service health alert**.
3. Enter the **Conditions**, **Actions**, and **Alert rule details** as desired.
4. Once you have entered all the required information, select **Create alert rule**.

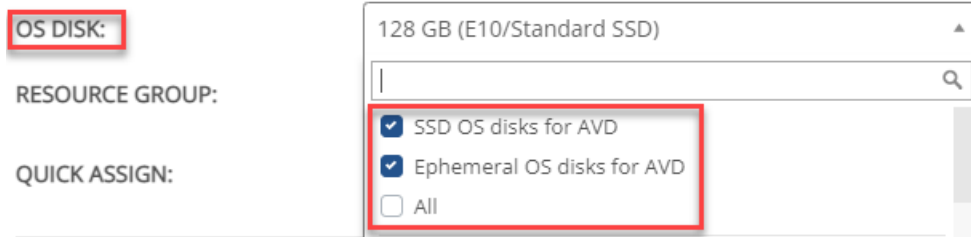
Resource Selection Rules Management

Nerdio Manager allows you to create recommendation and filtering rules to assist with the selection of VM sizes and OS disks when creating host pools or adding session host VMs.

Resource selection rules can be used to suggest the best VM for a specific AVD use-case, while taking into account core availability. They can also be used to limit the types of VMs and OS disks that can be used globally in a workspace, or even at the host pool level.

The VMs can be filtered based on vCPU availability in a selected subscription and region, processor, VM family & version, number of cores & GB of RAM, and local temp storage. OS disks can be filtered based on storage type (premium, standard, SSD, HDD, or Ephemeral) and disk size.

For example, when adding dynamic host pool, you can filter the **VM Size** or **OS Disk** choices by selecting the desired Resource Selection Rule(s).



Create a Resource Selection Rule

A resource selection rule must be created in order to use it for recommendations and filtering.

To create a resource selection rule:

1. Navigate to **Settings > Resources rules**.
2. Select **Add**.
3. Enter the following information:
 - **Name:** Type the rule's name.
 - **Description:** Type the rule's description.
 - **Scope:** From the drop-down list, select the scope of the rule.

Notes:

- **Show if no explicit rules:** Display this rule's selection in all VM size and OS disk drop-down lists unless a rule with an explicit scope applies.
 - **Show everywhere:** Display this rule's selections in all VM size and OS disk drop-down lists.
 - **Desktop images:** Display this rule's selections when working with VMs on the Desktop Images page.
 - **Temporary VMs:** Display this rule's selections when working with temporary VMs.
 - **Individual Workspace or Host Pool:** Only display this rule's selections for the selected workspace(s) or host pool(s).
-
- **Show costs:** From the drop-down list, select **Yes** to display the monthly cost, instead of the size tier, in the VM Size drop-down list.

Note: This only applies if this rule is the top selected one.

- **Selected by Default:** From the drop-down list, select **Yes** to automatically check this rule when opening any drop-down selection list where this rule applies. Select **No** and this rule is not automatically checked.
- **VM Size Drop-Down Selection Rules:** Toggle to define the VM size rules for filtering.
 - **Processor:** From the drop-down list, select the processor manufacturer.
 - **VM Family Version:** From the drop-down list, select the VM family version(s).
 - **VM Family Type:** From the drop-down list, select the individual VM families or use-case optimized VM families.
 - **Exclude VM Type:** From the drop-down list, select the excluded individual VM families.

- **CPU Cores:** From the drop-down list, select the number of CPU cores.

Note: All VMs that match the number of cores, or fall out in between the selection and next power of 2, are displayed. For example, selecting 4 cores matches VMs with 4 and 6 cores.

- **RAM (GB):** From the drop-down list, select the size of the RAM.

Note: All VMs that match the size of the RAM, or fall out in between the selection and next power of 2, are displayed. For example, selecting 4 GB RAM matches VMs with 4 and 6 GB of RAM.

- **Local Storage:** From the drop-down list, select whether the VMs have temporary local storage.

Note:

- **Yes:** Filter for VMs with local temporary storage.
- **No:** Filter for VMs without local temporary storage.

- **VM Availability:** From the drop-down list, select the availability type.

Note:

- **Based on subscription & region only:** Do not validate core quota allocation. Only ensure that the VM type is available in the selected subscription and region.
- **Based on CPU core quota:** Dynamically validate that there is sufficient core quota available in the selected subscription and region and only display those VMs that can be deployed.

- **Sort By:** From the drop-down list, select the sort criteria.

Note: **Alphabetical** is a stand-alone sort criteria. The other options can be combined.

- **Disk Size Drop-Down Selection Rules:** Toggle to define the disk size rules for filtering.
 - **Storage Type:** From the drop-down list, select the storage type(s).
 - **OS Disk Size:** From the drop-down list, select the disk size(s).

Note: For **Ephemeral OS disks**, the disk size may not match the exact selection. In such cases, the EOSD sizes that fall out in between the selection and the next power of 2 are displayed. For example, selecting 64 GB matches EOSD of 75 GB.

4. Once you have entered all the desired information, select **OK**.

The resource selection rule is created.

Manage Resource Selection Rules

From the Resource Selection Rules table, you can do the following:

- **Edit:** Edit the rule.

Note: Built-in rules cannot be edited. You need to copy the rule and edit the copy.

- **Clone:** Create a copy of the rule.
- **Disable:** Disable the rule.

Note: Disabled rules are not displayed on any drop-down selection lists.

- **Enable:** Enable a disabled rule.

- **Delete:** Delete the rule.
- **Change the Order:** Move the bands up and down as desired.

Note: This is the order the selections are shown in the drop-down boxes when creating a host pool or session host VM.

Manage Schedules for Tasks

Nerdio Manager supports the ability to configure schedules for tasks.

The schedule can contain one or multiple entries, as shown in these examples:

- You can create a schedule to power off a host today at 18:00.
- You can create a schedule to run the same scripted action on a host pool on Monday at 7:00 AM, Tuesday at 9:00 PM, and Sunday at 3:00 AM.
- You can create a schedule to restart hosts Monday and Thursday at 23:00 and have it recur every week.

Some of the functions that allow for multiple-entry schedules are:

- **Desktop Images:** Run scripted action
- **Scripted Actions:** Run Azure Runbook
- **Host Pools:** Resize or re-image, Power on/off, Restart hosts, Send message, Log off all hosts, Activate/Deactivate hosts, Run scripted action
- **Session Hosts (Excluding hybrid):** Resize or re-image, Power on/off, Restart hosts, Send message, Activate/Deactivate hosts, Run scripted action
- **Advisor:** Resize session host, Resize host pool

Create Multiple Schedules for a Task

Nerdio Manager allows you to create multiple schedules for a number of tasks.

To create multiple schedules for a task:

1. Navigate to the task you wish to perform.

Note: In this example, we are restarting a session host. As noted above, multiple schedules can be created for a number of tasks.

2. Select the **Schedule** tab.

CONFIRM ACTION

SCHEDULE

Do you want to restart AATCH-DEMO-7ddc.nerdio.int?

Log off users

Send a message to all users on a session host before performing the operation. Session hosts will be placed into drain mode (deactivated) before the message is sent.

MESSAGING ⓘ

Delay: ⓘ

Message:

The task will be performed according to the specified schedule.

SCHEDULE ⓘ

Start date: ⓘ

Time zone: ⓘ

Start time: ⓘ : ⓘ

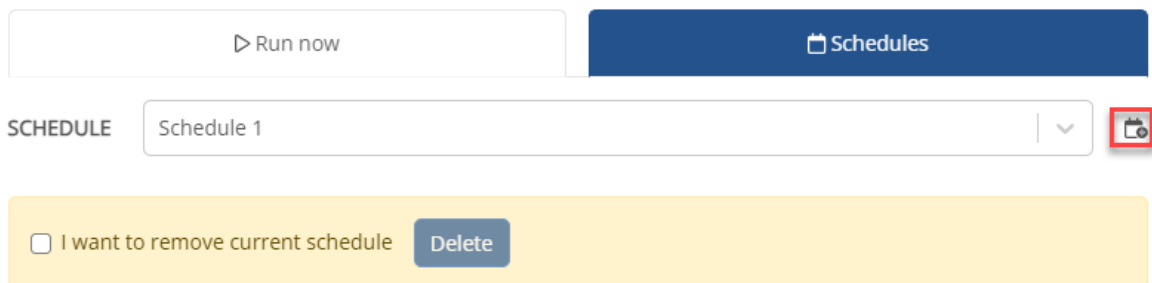
Repeat: ⓘ

3. In the **Schedule** section, enter the desired schedule.

- **Start Date:** Type the date to start.
- **Time Zone:** From the drop-down list, select the time zone for the Start time.
- **Start Time:** From the drop-down lists, select the time to start.
- **Repeat:** From the drop-down list, select whether to run this operation once or repeat it on a recurring schedule.


Note: The drop-down has the option **After Patch Tuesday**. This allows you to create a recurring schedule based on [Patch Tuesday](#).

- **Day of Week:** From the drop-down list, select the day for the recurring schedule.
 - **Days After:** If you selected **After Patch Tuesday**, type the number of days after Patch Tuesday to run the scheduled task.
4. Once you have entered the schedule, select **Save**.



The screenshot shows a user interface for managing task schedules. At the top, there are two buttons: a white 'Run now' button with a play icon and a blue 'Schedules' button with a calendar icon. Below these is a 'SCHEDULE' dropdown menu with 'Schedule 1' selected and a red-bordered 'Add Schedule' icon to its right. At the bottom, there is a yellow banner with a checkbox labeled 'I want to remove current schedule' and a blue 'Delete' button.


Schedule 1 is added to the task.



5. If you want to add additional entries, at the top, to the right of **Schedule**, select the **Add Schedule** icon. 
6. Add and save the next schedule, and repeat for all the desired schedule entries.

Manage Task Schedules


Nerdio Manager allows you to manage task schedules. This includes changing and deleting schedule entries.

To manage task schedules:

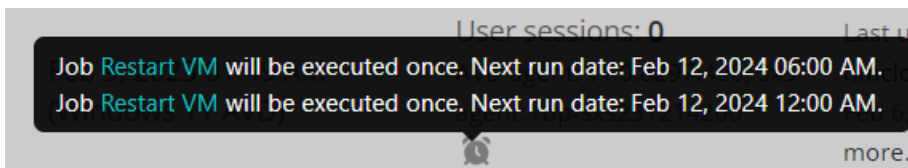
1. Navigate to the task with the schedule that you wish to work with.
2. On the list (for example, hosts, host pools, etc.), select the **Schedule** icon. 

STATUS  

User sessions: 0
AVD agent: v1.0.8297.400, SxS
agent: rdp-sxs231214200





3. In the schedule list, select the schedule you wish to work with.



4. Change or remove the schedule entry as desired.
5. Alternatively, open the task (for example, restart a session host) and in the **Schedule** tab, from the drop-down list, select the schedule entry you wish to change or remove.

CONFIRM ACTION

SCHEDULE  

I want to

- Schedule 1
Once. Next run date: Feb 12, 2024 06:00 AM.
- Schedule 2
Once. Next run date: Feb 12, 2024 12:00 AM.

6. Once you have made the desired changes, select **Save**.

UI overview

Nerdio Manager's UI is feature rich and customizable.


Time Zone

Nerdio Manager displays all date and time information in your local time zone as indicated by your browser. Please check your browser settings or your personal device settings if the time zone in Nerdio Manager seems incorrect.


Menu

Select the **Menu** icon  to expand and collapse the main menu.

Help

Select the **Help** icon  to display the Nerdio Manager help center.

Nerdio Manager Copilot

Select the **Copilot** icon  to launch the AI-assisted help system. See "Manage Nerdio Manager Copilot" on page 112 for details.

Breadcrumbs

You can select anywhere on the breadcrumbs to return to an earlier page in your navigation flow. For example:

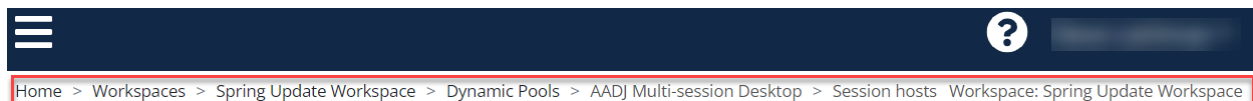
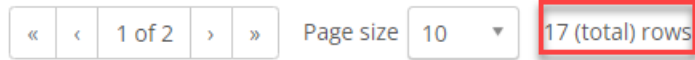



Table Footer

Many tables have footers that allow you to quickly navigate through the table and set the page size. In addition, some tables show the total number of rows in the table.



Tasks

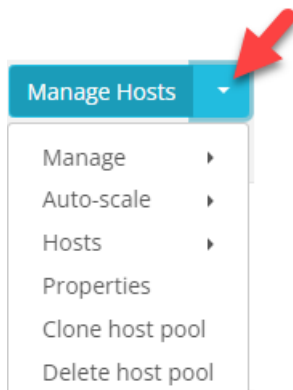
The **Tasks** section displays a log of the tasks related to the page in reverse chronological order. For example, the Workspaces page displays the log of the tasks performed on the Workspaces.

Select either of the export buttons  to export the tasks table in JSON or CSV format.

See "Logs Module" on page 368 for details.

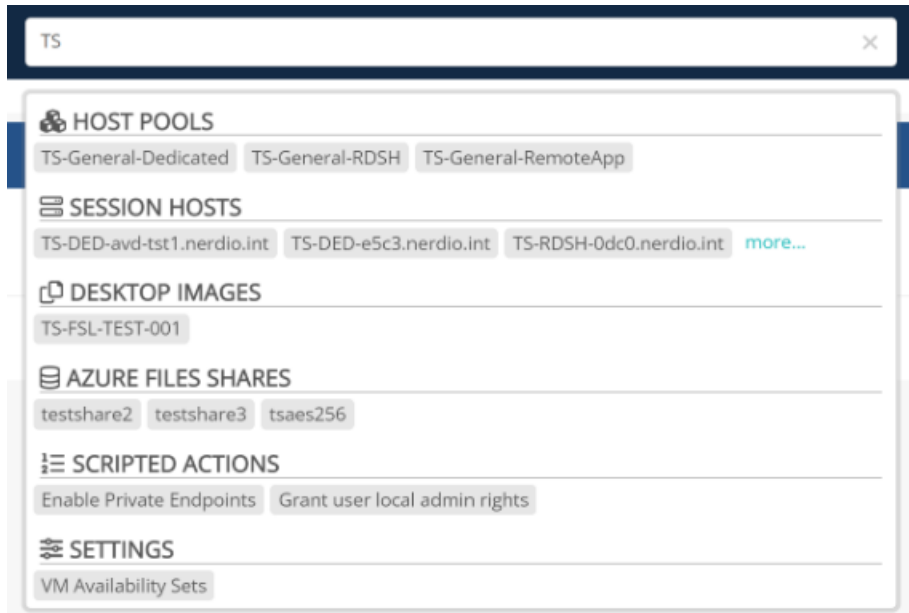
Action Menu

Several pages have an **Action Menu** on each row in the table. For example, the Dynamic Host Pools page, select the **down** arrow to view the Action Menu.



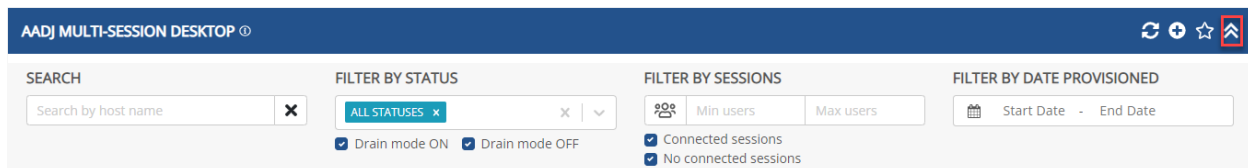
Global Search Bar

At the top of every page, the Global Search bar allows you to search for resources, objects, and settings, and to quickly navigate to your desired location.





Search and Filter


Many pages have search and filter features that allow you to quickly find the information you are looking for. For example, the Session Hosts page can be searched and filtered as follows:




Notes:

- Select the search/filter display toggle icons   to toggle the search/filter section of the page on or off.
- Use built-in search field on all pages to filter items displayed in the table. For example, you can find hosts using a specific image. The search matches are highlighted.
- You can search for “not contains” strings. For example, you can search for hosts that do not contain “avd” in the name by searching for “-avd”.


Refresh

Select the **Refresh** icon  to refresh the table that is displayed.


Tool Tip

Select the **Tool Tip** icon  to see a pop-up window with valuable information about the field the tool tip is associated with.


Sort a Table

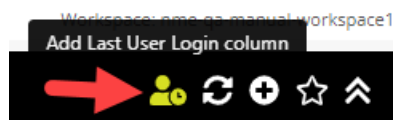
In a table column header, select the **Sort** icon  to sort the table in ascending or descending order by that column.

Add New

Where applicable, select the **Add New** icon  to add a new item. For example, to add a new session host or a new provisioning policy.

Display Last Login Date

Where applicable, you can display the last login for session host VMs or user sessions. In the upper right corner, select the **Add Last User Login column** button. 



Multi-select and Bulk Actions

On many lists, Nerdio Manager allows you to make multiple selections from the list and perform bulk actions on the items selected. As shown below, 3 session hosts were selected and you can perform bulk actions, such as power on, on the 3 session hosts.

Note: You may make multiple selections over multiple pages. For example, you may select 2 session hosts on the first page and 4 session hosts on the third page. The bulk action is performed on the 6 session hosts.

The screenshot shows the 'AADJ MULTI-SESSION DESKTOP' page. At the top, there are search and filter options. Below, a table lists three VMs, each with a 'Power on' button. A red box highlights the first three rows of the table. Below the table, a '3 items (3 selected)' indicator is visible. A 'select bulk action' dropdown menu is open, showing options like 'Resize/Re-image selected (3)', 'Power on selected (3)', 'Exclude from autoscale selected (3)', 'Deactivate selected (3)', 'Delete selected (3)', and 'Run script on selected (3)'. Below the table, there is a 'HOST POOL TASKS' section with a table showing task details for 'Activate session host'.

NAME	VM	PROVISIONED	STATUS	LAST USER LOGIN	
AADJMS-28e8 (Entra ID joined) 10.1.254.48 (NWM-Demo-Vnet/NWM/northcentralus/AN)	VM size: D2s_v3 (2C & 8GB) OS disk: 128 GB (S10/Standard HDD) Resource group: NWM-DEMO	Jun 21, 2024 01:56 PM	User sessions: 0 AVD agent: v1.0.9742.1900, SxS agent: rdp-sxs240705700	N/A	Power on
AADJMS-Q264 (Entra ID joined) 10.1.254.35 (NWM-Demo-Vnet/NWM/northcentralus/AN)	VM size: D2as_v5 (2C & 8GB) OS disk: 128 GB (S10/Standard HDD) Resource group: NWM-DEMO	May 8, 2024 01:03 PM (Windows 11 AVD + Microsoft 365 Apps)	User sessions: 0 AVD agent: v1.0.9742.1900, SxS agent: rdp-sxs240705700	N/A	Power on
AADJMS-df60 (Entra ID joined) 10.1.254.53 (NWM-Demo-Vnet/NWM/northcentralus/AN)	VM size: D2s_v3 (2C & 8GB) OS disk: 128 GB (S10/Standard HDD) Resource group: NWM-DEMO	May 8, 2024 01:34 PM (Windows 11 AVD + Microsoft 365 Apps)	User sessions: 0 AVD agent: v1.0.9742.1900, SxS agent: rdp-sxs240705700	N/A	Power on

TASK	RESOURCE NAME	USER	STATUS	CREATED	COMPLETED
Activate session host	AADJMS-28e8	<Automatic task>	COMPLETE	Oct 13, 2024 06:08 PM	Oct 13, 2024 06:09 PM

Custom Views

Nerdio Manager allows administrators to create custom views that best represents their workflows. Multiple views can be created and one of the views can be designated as the default view.

For example, if you manage host pools across several Workspaces, there is no need to keep jumping back to the Workspaces list to switch from one Workspace to the next to work with all the host pools. With custom views, you can combine similar data on a single page across the environment.

See "Create a custom view" on page 102 for details.

Custom Views based on an Existing Page

Nerdio Manager allows administrators to create a custom view from an existing page. For example, you may be viewing a filtered list of host pools and you want to save the page as a custom view.

See "Create a custom view from an existing page" on page 109 for details.

Individualize Your UI Themes

Nerdio Manager allows you to individualize your UI themes.

See "Individualize your UI themes" on the next page for details.

Summary Dashboard

Nerdio Manager's Summary Dashboard displays summary information about usage and savings in all the workspaces or AVD tenants. The Summary Dashboard allows you to view the summary information, drill down to view details, and export usage and savings data in a CSV file.

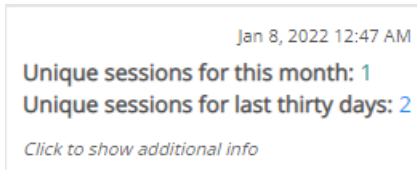
To view the summary dashboard:

1. Navigate to **Dashboard**.
2. Select either **All workspaces** or **All AVD tenants**.
3. In **Time Range**, select the desired time range to display.

The following information is displayed:

- **Auto-Scale Savings:** This is the savings from auto-scaling over the selected period of time. The costs are based on Azure pay-as-you-go list prices. Static host pool information is not included.
 - **Savings:** Select the information icon ⓘ to see host pool, file share, and NetApp Files savings information.
 - **Named user cost:** This is the projected per-named user monthly cost taking into account the auto-scale savings. This is based on Azure pay-as-you-go list prices.
 - **Concurrent user cost:** This is the projected per-concurrent user monthly cost taking into the account auto-scale savings. This is based on Azure pay-as-you-go list prices.
 - **Monthly active user cost:** This is the calculated active user monthly cost taking into account auto-scale savings. This is based on Azure pay-as-you-go list prices. Static host pool information is not included.

- **Current Host Pools Counts:** This is a summary of the host pools and session hosts, broken down by the type of desktop experience.
- **Hover:** You can hover over any part of any graph to see its details. For example:



- Select any point on any graph to display the **Usage Details** window. These are the details for the Workspaces or Tenants at the selected point in time.
- Select **Export details** to export a usage details CSV file to your browser's default download folder.
- **Select export:** At the bottom of the dashboard, select **Select export** to export the desired report as a CSV file into your browser's default download folder.

Individualize your UI themes

Nerdio Manager allows you to individualize your UI themes.

Note: Prior to version 3.2, this was a global setting and any themes that were created prior to version 3.2 stay exactly as is. Starting with version 3.2, any changes to the themes only apply to the individual user.

To individualize your UI themes:

1. Navigate to **Settings > Theme**.
2. Enter the following information:
 - **Enable personal theme:** Select this option to allow users to create personal, customized themes. Unselect this option to force a global UI theme for all users as defined by an administrator and prohibit users from configuring personal themes.

- **(1) Themes:** From the drop-down list, select one of the preconfigured themes or **Custom**.
- For the **Custom** theme, modify the other sections as desired.

Note: You can do no harm by individualizing your theme, so experiment as much as you want. You can always revert back to one of the preconfigured themes.

3. Once you have entered all the desired changes, select **Apply**.

Create a custom view

Nerdio Manager allows administrators to create custom views that best represents their workflows. Multiple views can be created and one of the views can be designated as the default view.

For example, if you manage host pools across several Workspaces, there is no need to keep jumping back to the Workspaces list to switch from one Workspace to the next to work with all the host pools. With custom views, you can combine similar data on a single page across the environment.

Note: You can run bulk actions like **Run script**, **Restart**, and **Power off** on session hosts in custom views.

To create custom views:

1. Navigate to **Settings > Custom views**.
2. Select **Add custom view**.
3. Enter the following information:
 - **Name:** Type the custom view's name.
 - **Description:** Type the description of the custom view.

- **Type:** From the drop-down list, select the type of information you want to see in the custom view.

Note: The following types are available -- host pools, session hosts, user sessions, schedule configs, remote apps, desktop images, and Intune devices. Each type has different customization options, as explained below.

- **Visible To:** From the drop-down list, select who should be able to see this custom view.

Note: You can make this custom view visible to any of the following:

- Only you.
 - Everyone.
 - Users assigned to built-in roles.
 - Users assigned to custom roles.
- **Sort by Column:** From the drop-down list, select the column in the table to sort the contents by.
 - **Sort Direction:** From the drop-down list, select the sort direction.
 - **Page Size:** From the drop-down list, select the page size for the custom view.
 - For **Host pools**, enter the following information:

WORKSPACE SCOPE: x | v ⓘ

HOST POOL TYPE: ⓘ

DESKTOP EXPERIENCE: x | v ⓘ

SEARCH: ⓘ

RESOURCE GROUP: x | v ⓘ

- **Workspace Scope:** From the drop-down list, select the workspaces to include in the custom view. The default is **Any**.
 - **Host Pool Type:** From the drop-down list, select whether the custom view is for dynamic or static host pools.
 - **Desktop Experience:** From the drop-down list, select the desktop experience (s) of the host pools that should be displayed in the custom view.
 - **Search:** Optionally, type the search string to limit the results of the items displayed in the custom view.
 - **Resource Group:** From the drop-down list, select which resource group(s) should be included in the custom view. The default is **Any**.
- For **Session hosts**, enter the following information:

WORKSPACE SCOPE: x | v ⓘ
 HOST POOL SCOPE: x | v ⓘ
 SEARCH: ⓘ
 STATUS: x | v ⓘ
 Drain mode ON
 Drain mode OFF
 SESSIONS: ⓘ
 Connected sessions
 No connected sessions
 DATE PROVISIONED: ⓘ

- **Workspace Scope:** From the drop-down list, select the workspaces to include in the custom view. The default is **Any**.
 - **Host Pool Scope:** From the drop-down list, select the host pools to be included in the custom view within the selected workspaces. The default is **Any**.
 - **Search:** Optionally, type the search string to limit the results of the items displayed in the custom view.
 - **Status:** From the drop-down list, select the statuses to be included in the custom view. The default is **All Statuses**.
 - **Drain Mode:** Select these options to include the desired drain mode of session hosts.
 - **Sessions:** Indicate if you want to include session hosts with sessions and the number of user sessions.
 - **Date Provisioned:** Optionally, filter by the date session hosts were provisioned.
- For **User sessions**, enter the following information:

WORKSPACE SCOPE: ⓘ
 HOST POOL SCOPE: ⓘ
 SEARCH: ⓘ
 SESSION STATUS: Show Active user sessions ⓘ
 Show Disconnected user sessions ⓘ

- **Workspace Scope:** From the drop-down list, select the workspaces to include in the custom view. The default is **Any**.
 - **Host Pool Scope:** From the drop-down list, select the host pools to be included in the custom view within the selected workspaces. The default is **Any**.
 - **Search:** Optionally, type the search string to limit the results of the items displayed in the custom view.
 - **Session Status:** Select the desired user session statuses to include in the custom view.
- For **Scheduled configs**, enter the following information:

SEARCH BY RESOURCE: ⓘ
 FILTER BY RESOURCE AND TASK TYPE: ⓘ
 FILTER BY SCOPE: ⓘ
 FILTER BY NEXT RUN DATE: ⓘ

- **Search by Resource:** Optionally, type the resource name to limit the results of the items displayed in the custom view.
- **Filter by Resource Type and Task Type:** From the drop-down list, select the resource type and task type to be included in the custom view. The default is **Any**.
- **Filter by Scope:** From the drop-down list, select the scope to be included in the custom view. The default is **Any**.

- **Filter by Next Run Date:** From the drop-down list, select the next run date to be included in the custom view. The default is **All time**.
- For **Remote apps**, enter the following information:

WORKSPACE SCOPE: x | v ⓘ
 HOST POOL SCOPE: x | v ⓘ
 APP GROUP SCOPE: x | v ⓘ
 SEARCH: ⓘ
 TYPE: x | v ⓘ
 MAINTENANCE MODE: In maintenance ⓘ
 Not in maintenance

- **Search:** Optionally, type the search string to limit the results of the items displayed in the custom view.
- **Workspace Scope:** From the drop-down list, select the workspaces to be included in the custom view. The default is **Any**.
- **Host Pool Scope:** From the drop-down list, select the host pools to be included in the custom view within the selected workspaces. The default is **Any**.
- **Search:** Optionally, type the search string to limit the results of the items displayed in the custom view.
- **Type:** From the drop-down list, select the remote app types to be included in the custom view. The default is **Any**.
- **Maintenance Mode:** Select the maintenance modes to be included in the custom view.
- For **Desktop images**, enter the following information:

SEARCH: ⓘ
 TAG: x | v ⓘ

- **Search:**Optionally, type the search string to limit the results of the items displayed in the custom view.
- **Tag:**Optionally, type the tags to limit the results of the items displayed in the custom view.
- For **Intune devices**, enter the following information:

SEARCH: ⓘ

FILTER BY COMPLIANCE: x | v ⓘ

FILTER BY PLATFORM: | v ⓘ

FILTER BY FREE SPACE: x ⓘ

FILTER BY USER ASSIGNED: All Not assigned Assigned ⓘ

FILTER BY STATUS: x | v ⓘ

FILTER BY LICENSE: x | v ⓘ

- **Search:**Optionally, type the search string to limit the results of the items displayed in the custom view.
- **Filter by Compliance:** From the drop-down list, select the compliance statuses to be included in the custom view.
- **Filter by Platform:** From the drop-down list, select the platforms to be included in the custom view.
- **Filter by Free Space:** Type the free space range to be included in the custom view.
- **Filter by User Assigned:** From the drop-down list, select the assigned users to be included in the custom view.
- **Filter by Status:** From the drop-down list, select the statuses to be included in the custom view.

- **Filter by License:** From the drop-down list, select the license types to be included in the custom view.
 - **Set this view as the default page:** Select this option to automatically open this page when you launch Nerdio Manager
4. Once you have entered all the desired information, select **Save & close**.

The new custom view is now available at the top of the main menu.

Create a custom view from an existing page

Nerdio Manager allows administrators to create a custom view from an existing page. For example, you may be viewing a filtered list of host pools and you want to save the page as a custom view.

For detailed information about custom views, please see "Create a custom view" on page 102.

To create a custom view from an existing page:

1. Navigate to the page you wish to use as the template for the custom page.

Note: For example, navigate to the list of dynamic host pools for a particular workspace.

2. In the host pools example, type your search phrase, select the Filter By Types, select the Filter by Resource Group, etc.
3. Once the page displays the information you want, in the upper right side, select the edit custom view button.



Note: All the changes you made on the page are loaded in the edit window.

4. Type the **Name** of the new custom view.

5. Review all the options to confirm they are as desired and make any necessary changes.
6. Once you have entered all the desired information, select **Save & close**.

Change a custom view

Nerdio Manager allows administrators to change an existing custom view.

For detailed information about custom views, please see "Create a custom view" on page 102.

To change a custom view:

1. Navigate to **Settings > Custom views**.
2. In the **Custom views** section, select the custom view you wish to edit.
3. Make the desired changes and select **Save & close**.
4. Alternatively, when you are viewing a custom view page, make the changes you wish to save. For example, type a search filter.
5. In the upper right side, select the edit custom view button.



Note: All the changes you made on the custom view page are loaded in the edit window.

6. Review all the options to confirm they are as desired and make any necessary changes.
7. Once you have entered all the desired information, select **Save & close**.

Change custom views display properties

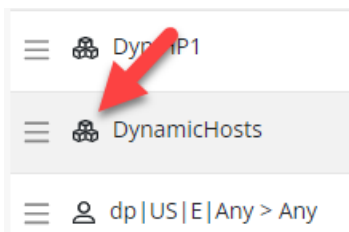
Nerdio Manager allows the administrators to change the following display properties of custom views.

- **Icon:** You can change the custom view's icon.
- **Display Order:** You can change the order the custom views are displayed on the main menu.
- **Grouping:** You may arrange multiple custom views under a single collapsible item called a group.

For detailed information about custom views, please see "Create a custom view" on page 102.


To change a custom view's icon:

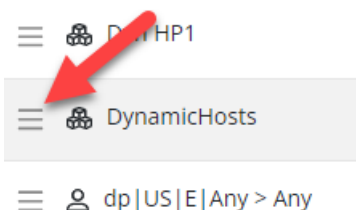
1. Navigate to **Settings > Custom views**.
2. Select the icon of the custom view you wish to change.



3. In the pop-up list of icons, select the new icon you wish to use.
4. Select **Confirm**.

To change a custom view's display order:

1. Navigate to **Settings > Custom views**.
2. Select and hold the custom view's .




3. Drag and drop the custom view to the desired location.

To create a group of custom views:

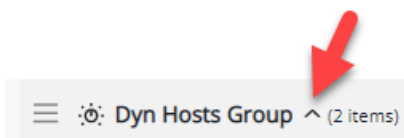
1. Navigate to **Settings > Custom views**.
2. Select **Add group**.
3. Select the new group's name to change it.



4. For each custom view you wish to add to the group, select and hold the custom view's , then drag and drop it under the group.

Note: You can remove a custom view from a group by dragging and dropping it outside the group.

5. Optionally, select **Sort** to sort the custom views within the group in ascending or descending order.
6. Optionally, select the group's icon to change it.
7. Optionally, select the **Up-Down arrow** next to the group's name to display or hide the custom views within the group.



Manage Nerdio Manager Copilot

Nerdio Manger Copilot leverages an AI-based assistant to quickly search for information about Nerdio Manager, its features, and functions.

Enable Nerdio Manager Copilot

Notes:

- Availability of Azure OpenAI services is limited and varies by Azure region.
- When enabling Copilot, you might have to register the following resource providers first or you might see this error message.

DEPLOY NERDIO MANAGER COPILOT ⓘ

Microsoft.BotService resource provider is not registered

- EventHub
- EventGrid
- BotService
- ServiceBus
- AppConfiguration
- Microsoft.Search

To enable Nerdio Manager Copilot:

1. In Nerdio Manager, navigate to **Settings** > **Nerdio environment**.
2. In the **Nerdio Manager Copilot** tile, select **Deploy**.

DEPLOY NERDIO MANAGER COPILOT ⓘ

Resource group ⓘ

Select resource group ▼

OpenAI: Please select regions for each required OpenAI model based on available quotas. You can choose the same region for all models or different regions for each model. A separate Azure resource will be created for each selected region.

Model name	Region
gpt-35-turbo	Select location ▼
gpt-4o	Select location ▼
gpt-4o-mini	Select location ▼
text-embedding-ada-002	Select location ▼

> Other Resources

> Customize resources tags ⓘ

Cancel

OK

3. Enter the following information:

- **Resource group:** From the drop-down list, select the resource group to contain all the resources required to run Nerdio Manager Copilot.
- **Model name- Regions:** From the drop-down lists, select the regions for each required OpenAI model based on available quotas.

Note: You may select the same region for all models or different regions for each model. A separate Azure resource is created for each selected region.

- **Other Resources:** Optionally, expand this to enter other resources.

Note: A partial list of **Other resources** is shown here:

▼ Other Resources	
TEXT TRANSLATION SERVICE	nerdio-copilot-text-translation-c23d
FORM RECOGNIZER SERVICE	nerdio-copilot-form-recognizer-c23d
<hr/>	
AD APPLICATION	nerdio-copilot-app-c23d
APP SERVICE PLAN LINUX	ASP-nerdiocopilot-linux
STORAGE ACCOUNT	nerdiocopilotsac23d
STORAGE ACCOUNT FUNC	nerdiocopilotfuncc23d
STORAGE ACCOUNT PY FUNC	nerdiocopilotpyfuncc23d

- **Customize resources tags:** Optionally, expand this to enter custom tags.
4. Once you have entered all the desired information, select **OK**.

The deployment task starts and takes about 30-35 minutes depending on the Azure region and other conditions. You can follow the task's progress in the **Settings Tasks** section.

Use Nerdio Manager Copilot

Once all Azure resources for Copilot are deployed, you may use Copilot.

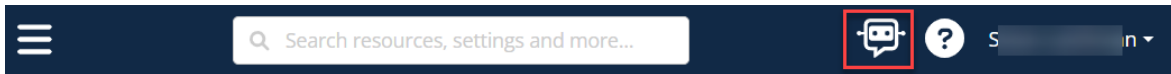
Note: Nerdio Manager Copilot caches the Nerdio Help Center KBs to answer your questions and refreshes the cache on a daily basis.

To use Nerdio Manager Copilot:

1. In the upper-right corner of Nerdio Manager, select the **Nerdio Manager Copilot** icon.



Nerdio Manager connects to the bot and downloads the chat history.



2. Users can ask any question related to Nerdio Manager and send them to Copilot. After a short period of time Copilot, displays an answer.

How do I change pool host configuration in NHY?

To change the host pool configuration in Nerdio Manager (NHY), you can customize the RDP settings by following these steps:

Locate the host pool you wish to work with.
From the action menu, select Properties > Custom RDP.
Enter the desired configuration and edit mode.
Save your changes **1**.

For FSLogix settings, navigate to the list of host pools, select the desired host pool, and then choose Properties > FSLogix to customize the settings **2**.

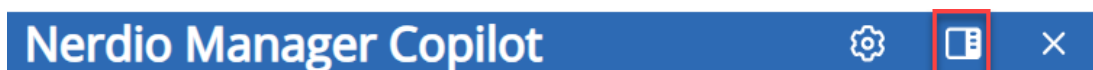
[Citations](#)

Just now

3. Optionally, select **Citations** to view a list of cited Knowledge Base articles.

4. You may select any of the view options:

- Switch to Sidebar window:



- Switch to Detached window:



Manage Nerdio Manager Copilot's chat settings

You may manage Copilot's settings at any time.

To manage Nerdio Manager's Copilot's chat settings:

1. Select the **Settings** icon. 

Chat Settings

Use rewriting for conversation context:

Yes

No

History count:

0

Intent recognition service OpenAI Model:

gpt-35-turbo

CANCEL

SAVE

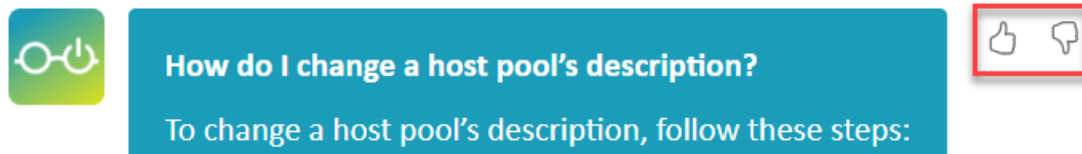
2. Enter the following information:
 - **Use rewriting for conversation context:** Select **Yes** or **No**.
 - **History count:** Type the number of chat histories to retain.
 - **Intent recognition service OpenAI Model:** From the drop-down list, select the desired model.
3. Once you have entered the desired information, select **Save**.
4. When prompted, select **Confirm** to confirm your changes.

Submit feedback

Copilot uses Azure OpenAI, powered by Large Language Model (LLM) that has been augmented with Nerdio-specific information. Due to this being an LLM, answers are not deterministic. See the following Microsoft [article](#) for more details.

When you notice an incorrect answer, you can submit feedback in the following ways:

- Select the **Like** or **Unlike** icon near the answer.



- Enter a comment (optional).
- Follow Nerdio's standard support escalation path.

Disable Nerdio Manager Copilot

Follow this procedure to disable Nerdio Manager Copilot.

Note: Disabling Nerdio Manager Copilot removes all the Azure resources that were deployed when the feature was enabled, except for the **Smart detector alert rule**.

To disable Nerdio Manager Copilot:

1. In Nerdio Manager, navigate to **Settings** > **Nerdio environment**.
2. In the **Nerdio Manager Copilot** tile, select **Disable**.

DISABLE NERDIO MANAGER COPILOT

Following resources will be removed

Storage account : [nerdiocopilotsa72a0](#)
Storage account : [nerdiocopilotfunc72a0](#)
Storage account : [nerdiocopilotpyfunc72a0](#)
Event Grid System Topic : [nerdiocopiloteg-72a0](#)
Event Hubs Namespace : [nerdio-copilot-event-hubs-72a0](#)
Event Hubs Namespace : [nerdio-copilot-sa-eh-72a0](#)
Event Grid System Topic : [nerdiocopiloteg](#)
Service Bus Namespace : [nerdio-copilot-sb-ns-72a0](#)
Search service : [nerdio-copilot-search-72a0](#)
Recovery Services vault : [nerdiocopilotrsvault-72a0](#)
SQL Server : [nerdio-copilot-sql-server-72a0](#)
SQL Server : [nerdio-copilot-sql-db-72a0](#)
Log analytics workspace : [nerdiocopilotanalyticsworkspace-72a0](#)
Log analytics workspace : [CustomLogs](#)
Open AI : [nerdio-copilot-text-translation-72a0](#)
Open AI : [nerdio-copilot-form-recognizer-72a0](#)
Application insights : [nerdio-copilot-bot-72a0](#)
Application insights : [nerdio-copilot-functions-72a0](#)
Application insights : [nerdio-copilot-functions-python-indexer-72a0](#)
Application insights : [nerdio-copilot-searcher-72a0](#)
App Configuration : [nerdio-copilot-app-config-72a0](#)
Web application : [nerdio-copilot-python-functions-72a0](#)
Web application : [nerdio-copilot-functions-72a0](#)
Web application : [nerdio-copilot-bot-72a0](#)
Web application : [nerdio-copilot-searcher-72a0](#)
Bot Service : [nerdio-copilot-bot-72a0](#)
Open AI : [nc-openai-eastus2-72a0](#)
Open AI : [nc-openai-eastus-72a0](#)

Cancel

OK

3. When prompted, select **OK**.

The disable task starts and takes about 6-12 minutes depending on the Azure region and other conditions. You can follow the task's progress in the **Settings Tasks** section.

Build scripts with Nerdio Manager Copilot

Note: This feature is in **Public Preview**.

Nerdio Manager Copilot includes Script Pro, which allows you to build scripts with Copilot.

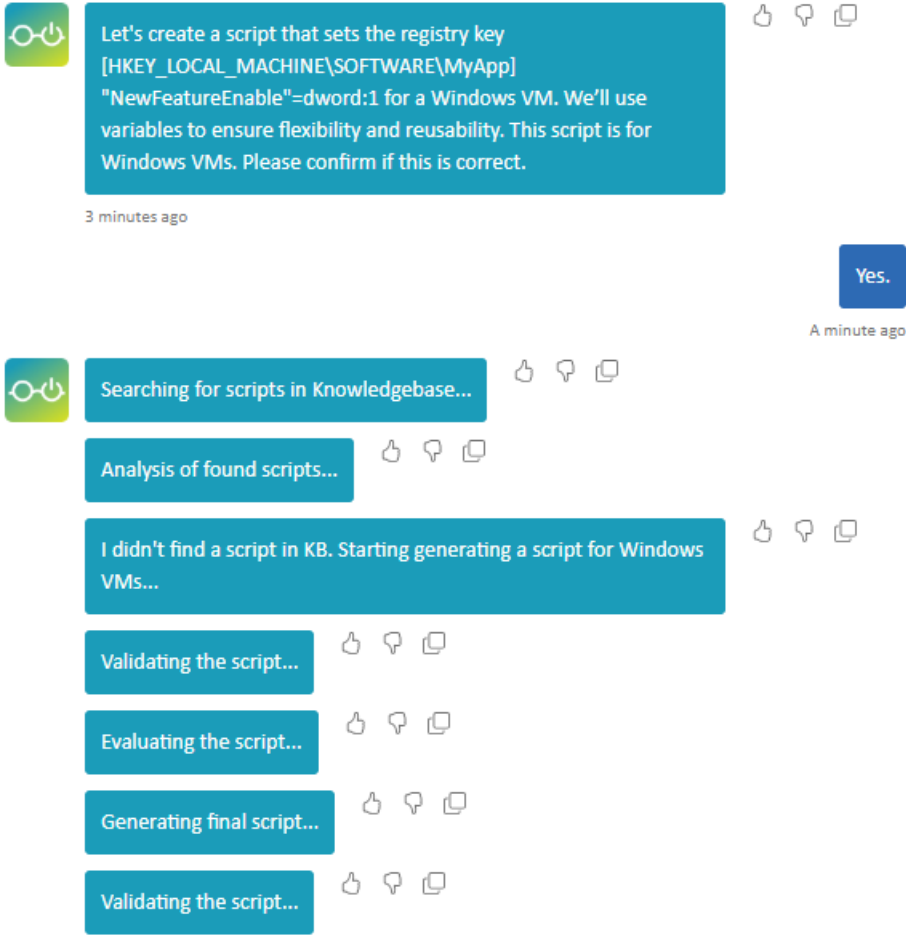
Warning: Ensure that all AI-generated scripts are tested and validated manually before deployment to your production environments.

To build a script with Nerdio Manager Copilot:

1. Open Nerdio Manager Copilot.
2. Ask a question related to building a script. For example:

```
Can you help me generate a management script for a Windows  
VM to set this regkey?  
[HKEY_LOCAL_MACHINE\SOFTWARE\MyApp]"NewFeatureEnable"  
=dword:1
```

3. Follow the prompts and reply as needed.



Let's create a script that sets the registry key [HKEY_LOCAL_MACHINE\SOFTWARE\MyApp] "NewFeatureEnable"=dword:1 for a Windows VM. We'll use variables to ensure flexibility and reusability. This script is for Windows VMs. Please confirm if this is correct.

3 minutes ago

Yes.

A minute ago

Searching for scripts in Knowledgebase...

Analysis of found scripts...

I didn't find a script in KB. Starting generating a script for Windows VMs...

Validating the script...

Evaluating the script...

Generating final script...

Validating the script...

4. When the script is generated, copy the code.

Validating the script...

```
#description: Sets a specified registry key with a
given value
#tags: ChatGPT, Registry, Logging

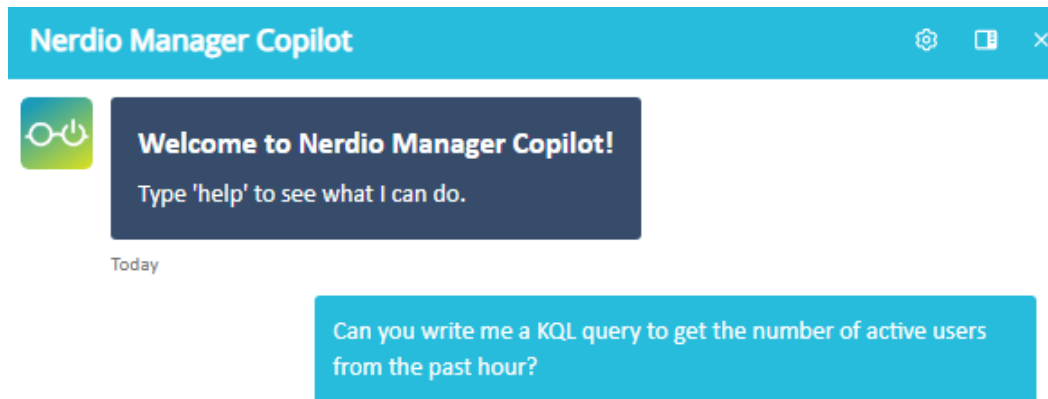
<#
variables: {
  "registryPath": {
    "description": "The registry path to
modify",
    "required": true
  },
  "registryName": {
    "description": "The registry key name to
set",
    "required": true
  },
  "registryValue": {
    "description": "The value to set for the
registry key",
    "required": true
  }
}
#>
```


Generate KQL queries with Nerdio Manager Copilot AnalyticsPro

AnalyticsPro, is a powerful new tool within Nerdio Manager Copilot that transforms your natural language questions into Kusto Query Language (KQL) queries. With AnalyticsPro, you can effortlessly generate KQL queries that can be executed in your Azure Log Analytics workspace, unlocking valuable insights from your data without needing to master complex query syntax.

To generate a KQL query using AnalyticsPro:

1. Open Nerdio Manager Copilot.
2. Enter the details of the KQL query you want to generate. For example:



3. Select the send  icon.
4. The KQL query is generated



Generating KQL query...



Understanding the **User Query Intent**, the task is to craft a KQL query that identifies the number of active users within the last hour. "Active users" are defined here as those in a "Connected" state within the given timeframe.



Choice of Specific Tables and Fields is important:

Table: `WVDConnections` is chosen because it logs all connections, providing data on user activity and their connection states.

Fields:

State: It identifies whether the user is currently "Connected" or not.

TimeGenerated: It timestamps each connection event, allowing me to filter the data to the last hour.

UserName: It differentiates between individual users to enable counting distinct users.

KQL Query

```
WVDConnections
| where State == "Connected" // Filter for active
(connection) users
| where TimeGenerated >= ago(1h) // Filter for the
past hour
| summarize ActiveUserCount = dcount(UserName) //
Count distinct active users
```

Step-by-Step Reasoning Behind Construction of the KQL Query:

Filter for Active Connections:

`| where State == "Connected"`: This line filters the records to only include those where the connection's state is "Connected", ensuring that only active users are counted.

Time Constraint:

5. You can interact with AnalyticsPro and ask for additional information based on the results, or provide options to help refine your query. Respond to these prompts as needed to tailor the query to your specific requirements.
6. Once complete, you can copy the query and run it in your Azure Log Analytics workspace.

Warning: Ensure that all AI-generated queries are tested and validated manually before deployment to your production environments

Cost of Nerdio Manager Copilot

The estimated cost for Nerdio Manager Copilot when using out of the box, and with up to 5 users asking 5 questions per day, is about \$35 per month.

Copilot has the following paid components:

- Azure App Service
- Azure Event Grid
- Azure Event Hub
- Azure Service Bus
- Azure Search Service
- Azure SQL Server
- Azure Text Translation
- Azure Form Recognizer
- Azure OpenAI Services
- Azure Bot Service
- Azure Application Insights
- Azure Functions
- Azure App Configuration
- Azure Storage

Here are the details on how you can get the exact cost of Copilot:

- **App Service:** The price depends on the App Service plan that Nerdio Manager Copilot is using. The default plan is B2 (Linux). See the following Microsoft [article](#) for more details.
- **Azure OpenAI Service** This service's cost depends on usage of Copilot and the number of input and output tokens that are being used in each interaction. See the following Microsoft [article](#) for more details.
- **Azure AI Search:** Copilot uses the basic tier for this service that is priced at \$0.11 per hour , which is approximately \$80 per month. See the following Microsoft [article](#) for more details.
- **Azure Event Grid:** The Event Grid Basic tier is priced as pay-per-use based on operations performed. The detailed pricing info is [here](#).
- **Azure Event Hub:** The basic tier pricing starts from \$0.015/hour per Throughput Unit (about \$12/month). The detailed pricing info is [here](#).
- **Azure Service Bus:** The basic tier pricing starts from \$0.05 per million operations. The detailed pricing info is [here](#).
- **Azure SQL:** Standard service tier (S0), Max storage: 250 GB, which is about \$14.7187/month
- **Azure App Configuration:** In Standard tier, this service charges \$1.20 per store per day, plus an overage charge at \$0.06 per 10,000 requests. The monthly charge expects to be no more than \$36. See the following Microsoft [article](#) for more details.
- **Azure Text Translation:** This uses tier S1 - Pay as you go (Standard Translation - \$10 per million characters, Custom Translation - \$40 per million characters). Here is the [pricing page](#).
- **Azure Form Recognizer:** This uses tier S0 - Pay as you go (minimal charge is: 0-1M pages - \$1.50 per 1,000 pages, 1M+ pages - \$0.60 per 1,000 pages). Here is the [pricing page](#).
- **Azure Bot Service:** The free tier is used. Detailed pricing info is [here](#).
- **Azure Functions:** The Azure Functions consumption plan is billed based on per-second resource consumption and executions. The detailed pricing page with calculation examples is [here](#).

- **Azure Storage:** Some of the components use Azure Storage. The cost of storage varies depending on the region and access tier selected, as well as the type of storage being used. Copilot uses Azure General Purpose v2 Storage Account, locally redundant storage (LRS). Here is the [pricing page](#).

Note: This is an estimate and not a guarantee of the cost. The Azure costs must be monitored.

Functional considerations

LLM implementation work with tokens. The number of tokens is a combination of system prompt, input from user, and output from LLM. The number of tokens defines how much “memory” about a previous exchange in the current conversation the bot has. If a conversation is long, larger than the max token count configured for the model, older data is dropped. However, we expose all the chat history in the UI until the chat history is deleted using the delete history button.

Deployment considerations

By default, Copilot deploys all resources in the same region, Azure OpenAI resources can be created in different regions, based on user’s selection. When possible and applicable, we deploy the free or the lowest paid tier resources, and that is not configurable..

Known limitations

- Users cannot control the throttling limit per day and/or month.
- There is no support for notifications.
- There is no mechanism for identifying and filtering out false positives.
- Smart detector alert rules are not deleted when Copilot is disabled.

Desktop Images

This section discusses topics related to desktop images. We will discuss the various import and lifecycle management options, as well as different ways to automate certain tasks in more advanced scenarios.

After creating a new Workspace, the next step in building out an AVD environment is to create one or multiple host pools housing your virtual machines (see "Host Pools" on page 204 for more information). Virtual machines are created based on a desktop image, which holds the operating system, your applications, and anything else you might want to add. For this to work, we first need to create at least one desktop image.

Before we continue, it is important to understand that images can be created or imported in different ways. Also note, that even when there are no images imported into Nerdio Manager, the custom Azure images part of your subscription can be used to build new host pools and re-image existing host pools in exactly the same way as with imported images. However, if you do choose to import your images into Nerdio Manager, you can take advantage of many different management features otherwise not available.

In addition, when images are imported into Nerdio Manager all of your management and lifecycle activities are done using a single management portal.

Once an image is created or imported, regardless of the type of image (we'll explain in more detail going forward), creating new host pools and re-imaging existing host pools is done in the same way. In the sections below we will walk you through it step by step.

Management and Lifecycle Tasks for Imported Desktop Images

No matter where your desktop images are imported from, their management and lifecycle tasks are the same.

Typical Desktop Image Lifecycle

1. Import the desktop image.

See any of the following for detailed information:

- "Import Images from the Azure Library" on page 131
 - "Import Custom Azure Managed Images" on page 136
 - "Import an Existing VM" on page 137
2. Power on the desktop image.
 - Navigate to **Desktop Images**.
 - Locate the desktop image you wish to power on.
 - Select **Power on**.
 - Optionally, select **Back up VM before powering on**.

Note: Selecting this option makes a backup of the desktop image VM before it is powered on, which creates a snapshot of the current configuration. The first backup process may take a long time.

The VM powers on.

3. Use the VM's IP address or name to connect to it using RDP and make all the desired changes.
4. Select **Power off & set as image**.

See "Desktop Images Set as Image" on page 140 for details.

Note: An extensive automation process begins that commits the changes to an image object. This includes many tasks you would have had to do manually like Sysprep and sealing the image.

You can see the job's progress in the logs. See "Desktop Images Change Log Feature" on page 154 for details about the logs.

5. Once the image is set, you can use it to build new host pools or re-image an existing host pool.

See the following for detailed information.

- "Create Dynamic Host Pools" on page 214
- "Create Static Host Pools Without Auto-Scaling" on page 206
- "Resize/Re-image a Host Pool" on page 270

Endpoint Management Software Integration

Nerdio Manager allows you to utilize the power of an endpoint management tool (for example, Microsoft's Endpoint Configuration Manager or Ivanti's Endpoint Manager) to leverage its power to work with Nerdio Manager.

Endpoint Management Software Integration Example

Patch Tuesday, when Microsoft releases its monthly software updates, occurs on the second Tuesday of each month at about 10 AM Pacific Standard Time. You can use your endpoint management tool, along with Nerdio Manager, to fully automate applying the Windows Updates to the desktop image and re-imaging the host pools with the updated desktop image.

Note: This is just one example of the many things you can do using these built-in automation tools.

- In Nerdio Manager, when you perform the **Set as image** function, be sure to select the **Leave desktop image VM running** option. This leaves the VM running after the **Set as image** task completes and the endpoint management tool can access the VM and change the image.
- In the endpoint management tool, create a recurring scheduled job/runbook on Patch Tuesday to apply the Windows Updates.
- In Nerdio Manager, configure the **Set as image** function for the desktop image to be a recurring job that starts shortly after the endpoint management tool's job completes. See "Desktop Images Set as Image" on page 140 for details about configuring the job.
- In Nerdio Manager, configure the **Re-image Hosts** function for the host pool to be recurring job that starts shortly after the **Set as image** process completes. See "Resize/Re-image a Host Pool" on page 270 for details about configuring the job.

So, by creating three recurring scheduled jobs you can apply the Windows Updates to the VM, set the VM image, and then update the host pool with the updated desktop image every month.

Import Images from the Azure Library

Nerdio Manager allows you to import a desktop image from the Azure library into a Workspace.

To import an image from the Azure library:

1. Navigate to **Desktop Images**.
2. Select **Add from Azure library**.
3. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 86 for details.

- **Name:** Type the desktop image's name.
- **Description:** Type the description.
- **Network:** From the drop-down list, select the network to which the VM connects.

Note: The VM is created in the Azure region associated with the network.

- **Azure Image:** From the drop-down list, select the desired image.

Note: Select the image based on the Windows OS supported by AVD. EVD = Enterprise Virtual Desktop (aka Windows 10 multi-session). Office Pro Plus contains a pre-installed Office 365 version of Pro Plus that is activated as users with appropriate licensing sign in to the desktop.

- **VM Size:** From the drop-down list, select the size.
- **OS Disk:** From the drop-down list, select the disk.
- **Resource Group:** From the drop-down list, select the resource group to contain the network interface cards of the VM.
- **Security type:** From the drop-down list, select the security option that best suits your desktop image VM.

Note:

- **Standard** is set by default. Additional security options are only available for generation 2 VMs with the **Geographic distribution & Azure compute gallery** option enabled.
- The **Trusted launch** and **Confidential virtual machines** security options help improve the security of Azure generation 2 virtual machines. However, additional security features they provide also have some limitations, such as the lack of support for backup, managed disks, and ephemeral OS disks. To learn more, see:
 - [Trusted launch for Azure virtual machines](#)
 - [About Azure confidential VMs](#)
- **Secure Boot:** Select this option to enable Secure Boot, which helps protect your VMs against boot kits, rootkits, and kernel-level malware.
- **vTPM:** Select this option to enable Virtual Trusted Platform Module (vTPM), which is TPM 2.0 compliant and validates your VM boot integrity apart from securely storing keys and secrets.
- **Integrity Monitoring:** Select this option to enable cryptographic attestation and verification of VM boot integrity along with monitoring alerts if the VM didn't boot because the attestation failed with the defined baseline.
- **OS State:** From the drop-down list, select the OS state.

Note:

- Generalized images have had the machine and user-specific information removed by running a command on the VM.
 - Specialized images have not been through the process to remove machine and user-specific information.
- **Join to AD:** Deselecting this means the VM is not joined to AD during the creation process. This prevents AD GPOs from applying to the image before it is created. Be sure to specify local administrator credentials below to be able to connect to the VM, since it won't be a member of the AD domain.
 - **Do not create image object:** Select this option to only create a desktop image VM but not create an image object.

Note: You need to create the image object. Select **Power off and set as image** after the VM is created before this desktop image can be used for session host creation. If you skip image creation, you can make changes to the VM before it is converted to an image.

- **Skip removal of local profiles:** Select this option to bypass this step and not remove local user profiles before running Sysprep.

Note: During the image creation process, Nerdio Manager removes all local user profiles. This increases the likelihood of Sysprep success. Selecting this option bypasses this step. If there are any partially installed APPX apps on the image VM, Sysprep will fail to remove them.

- **Enable time zone redirection:** Select this option to enable time zone redirection on the image. This allows each user to see their local device's time zone inside of their AVD desktop session.

- **Set time zone:** Select this option to set the time zone of the VM and then, from the drop-down list, select the time zone.
- **Install MSIX app attach certificates:** Select this option to install all the stored certificates on the VM, if applicable.

Note: To view the stored certificates, navigate to **MSIX App Attach > Certificates**.

- **Optimize disk type when desktop image is stopped:** Select this option to downgrade the OS disk type when the desktop image is stopped in order to save money. When the VM starts, the OS disk type are changed back to the selected one.
- **Provide custom credentials for a local administrator user:** Toggle this option on to enter the username and password.
- **Geographic distribution & Azure compute gallery:** Select this option to store the image in Azure Compute Gallery and automatically distribute it to the selected Azure regions.
 - **Azure Compute Gallery:** From the drop-down list, select an existing Azure Compute Gallery or create a new one.

Note: Only one Azure Computer Gallery can be selected. The existing Azure Compute Gallery must be in a linked resource group in the same Azure subscription as the image VM.

- **Azure Regions:** From the drop-down list, select Azure regions where the Desktop Image version should be replicated.

Note: The current Azure region must be part of the selection.

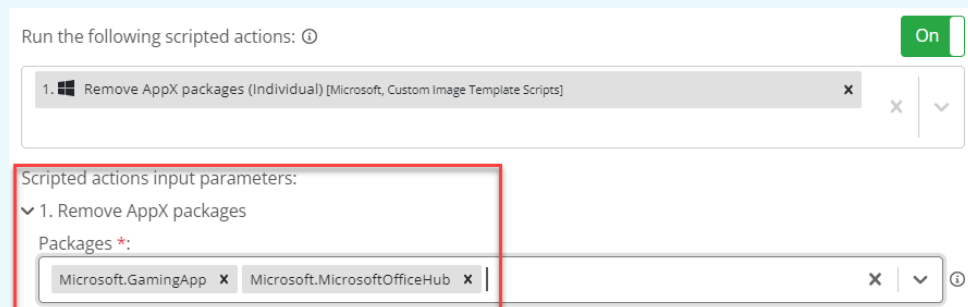
- **Custom (Stack HCI) Locations:** From the drop-down list, select custom locations where the desktop image should be replicated.
- **Replica Count (Per Region):** Type number of replicas per region.

Note: Azure Compute Gallery replicas support a maximum of 20 concurrent clone operations per replica. Ensure that the number of replicas specified meets your deployment requirements. Up to 100 replicas per region are supported. Replicas may only be deployed within the same subscription.

- **Run the following scripted actions:** Toggle this option on to specify the scripts that run during creation.

Notes:

- Windows scripts are executed via the Azure Custom Script extension and run in the context of LocalSystem account on the clone of the desktop image VM before it is Sysprep'ed. These commands do not run on the image VM itself.
- Azure runbooks are executed via the Azure automation account and run in the context of Nerdio Manager app service principal.
- Several variables are passed to the script and can be used in the PowerShell commands.
- If necessary, provide the required parameters. For example:



- **Applications Management:** Toggle this option on to specify the applications to deploy during creation.
 - **Applications:** In the applications list, select **Add new application**, and then from the drop-down list, select the application to include in this policy.

Notes:

- You may add as many applications as desired.
 - Drag and drop an application in the list to change its order on the list.
 - Select the "X" next to an application to remove it from the list.
- **Install/Uninstall:** Select whether the deployment policy should install or uninstall the selected applications.
 - **Reboot after installation:** Select this option to place the host in drain mode and restart it when no sessions are present.
 - **Show favorites only:** Select this option to only display applications marked as favorites. Otherwise, you may search the list of applications.
- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag.

Note: You may specify multiple tags. The specified tags are applied to image VM, OS disk, network interface, image object, and Azure Compute Gallery image. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

4. Once you have entered all the desired information, select **OK**.

The desktop image is created. This may take up to an hour to complete.

Import Custom Azure Managed Images

Nerdio Manager allows you to leverage your customized and managed Azure images and deploy them directly into Nerdio Manager.

To import an Azure custom image:

1. Navigate to **Desktop Images**.
2. Select **Add from Azure library**.

3. Enter the following information:

- **Azure Image:** From the drop-down list, select the desired image.

Note: The list contains all the standard Azure Marketplace images. In addition, it contains all the custom images that are available inside your Azure subscription.

Tip: Hover over any unavailable (grayed out) custom image to see why it is unavailable.

- Enter the information for the other fields. See "Import Images from the Azure Library" on page 131 for detailed information.

4. Once you have entered all the desired information, select **OK**.

The desktop image is created. This may take up to an hour to complete.

Import an Existing VM

You can import an existing VM as an image into Nerdio Manager. For example, you can take a custom VM from another virtual desktop deployment, that has all your applications installed, and use it as a custom image in your Nerdio Manager AVD deployment.

Note: In order for this to work, your VM needs to be based on a Managed Disk. That is, you need to generate the accompanying SAS URL directly from the Azure portal, as explained below.

To import an image:

1. In Azure, navigate to the virtual machine.

Warning: Make sure that the VM is powered off.

2. Navigate to **Settings > Disks**.
3. Select the OS disk and then select **Disk Export**.
4. Select **Generate URL**.

The URL is generated.

5. Copy the generated URL to the clipboard.
6. In Nerdio Manager, navigate to **Desktop Images**.
7. Select **Add from Azure VM**.
8. Enter the following information:

- **SAS URL:** Paste the URL from the clipboard.
- **Create image VM as Gen2:** Select this option to create the VM as Gen2.

Note: By default, desktop image VMs are created as Gen1. See this [Microsoft document](#) to learn more about the differences between Gen1 and Gen2 VMs.

- **Security Type:** From the drop-down list, select the security type.

Notes:

- Security type refers to the different security features available for a virtual machine. Security features like Trusted Launch and Confidential virtual machines improve the security of Gen2 VMs. However, additional security features have some limitations, which include not supporting back up, managed disks, and ephemeral OS disks. See the following Microsoft articles for more information:
 - [Trusted launch for Azure virtual machines](#)
 - [About Azure confidential VMs](#)
 - If you select **Standard**, **Trusted launch virtual machines**, or **Confidential virtual machines**, then the desktop image and session host VMs are created with the specific security type.
 - If you select one of the **xxxx supported** options, then the desktop image is created as Standard but the session host VMs can be deployed as Standard or the supported type(s). (Trusted Launch and/or Confidential)
- **Uninstall FSLogix app:** Select this option if the FSLogix app is already installed in the base image and you want to remove it in order to allow Nerdio Manager to manage FSLogix.
- **Uninstall AVD agent:** Select this option if you are creating an image from an existing AVD session host where the AVD agent has been previously installed.
- Enter the information for the other fields. See "Import Images from the Azure Library" on page 131 for detailed information.

9. Once you have entered all the desired information, select **OK**.

The desktop image import task starts.

Tip: Be sure to uninstall the AVD agent before you set this imported VM as a desktop image. See "Desktop Images Manually Uninstall AVD Agent" on page 146 for details.

Desktop Images Set as Image

Nerdio Manager provides a powerful tool that performs an extensive automation process to commit the Desktop Image changes to an image object. This includes many tasks you would have had to do manually like Sysprep and sealing the image. This would normally be done after you have made the updates to your image. Once you perform **Set as image**, the image object is created and is ready to be used either to build new host pools or to re-image existing host pools.

To set a desktop image:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to work with.
3. From the action menu, select **Power off & set as image** or **Set as image** (according to the power state of this desktop image).
4. Enter the following information:
 - **Run the following scripted actions before set as image:** Toggle on this option to run scripted action(s) before the set as image.

Note: For example, you can run scripts to optimize the image, install software, or install updates.

- From the drop-down menu, select the scripted action(s) you wish to run.
- **Pass AD credentials:** Select this option if you want to use them to run the scripted actions.
- **Applications Management:** Toggle this option on to specify the applications to deploy during creation.
 - **Applications:** In the applications list, select **Add new application**, and then from the drop-down list, select the application to include in this policy.

Notes:

- You may add as many applications as desired.
 - Drag and drop an application in the list to change its order on the list.
 - Select the "X" next to an application to remove it from the list.
-
- **Install/Uninstall:** Select whether the deployment policy should install or uninstall the selected applications.
 - **Reboot after installation:** Select this option to place the host in drain mode and restart it when no sessions are present.
 - **Show favorites only:** Select this option to only display applications marked as favorites. Otherwise, you may search the list of applications.
-
- **Schedule:** Toggle on the Schedule to perform the operations at a selected time(s). See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Security type:** From the drop-down list, select the security option that best suits your desktop image VM.

Note:

- **Standard** is set by default. Additional security options are only available for generation 2 VMs with the **Geographic distribution & Azure compute gallery** option enabled.
- The **Trusted launch** and **Confidential virtual machines** security options help improve the security of Azure generation 2 virtual machines. However, additional security features they provide also have some limitations, such as the lack of support for backup, managed disks, and ephemeral OS disks. To learn more, see:
 - [Trusted launch for Azure virtual machines](#)
 - [About Azure confidential VMs](#)

- **OS State:** From the drop-down list, select the OS state.

Note:

- Generalized images have had the machine and user-specific information removed by running a command on the VM.
- Specialized images have not been through the process to remove machine and user-specific information.

- **Geographic distribution & Azure compute gallery:** Select this option to store the image in Azure Compute Gallery and automatically distribute it to the selected Azure regions.
 - **Azure Compute Gallery:** From the drop-down list, select an existing Azure Compute Gallery or create a new one.

Note: Only one Azure Computer Gallery can be selected. The existing Azure Compute Gallery must be in a linked resource group in the same Azure subscription as the image VM.

- **Azure Regions:** From the drop-down list, select Azure regions where the Desktop Image version should be replicated.

Note: The current Azure region must be part of the selection.

- **Custom (Stack HCI) Locations:** From the drop-down list, select custom locations where the desktop image should be replicated.
- **Stage new image as inactive:** Select this option to create the new image version without setting it as active.

Note: Any existing configurations continue to use the current version of the image. See "Stage Desktop Images" on page 157 for details about activating staged desktop images.

- **Save current image as a backup:** Select this image to retain the existing image as a standalone object and not overwrite it with the new one.

- **Note:** This image is not visible or manageable via Nerdio Manager, so be sure to delete it manually when it is no longer needed to avoid unnecessary Azure storage costs.

If the current image is stored in Azure Compute Gallery, it is retained with an older version number. If the image is not stored in Azure Compute Gallery, you can find it in Azure portal>Images. It is listed under "Custom images" in the Nerdio Manager image selector drop-down list.

- **Install MSIX app attach certificates:** Select this option to install all stored certificates on the image VM, if any.
- **Skip removal of local profiles:** Select this option to bypass removing all local user profiles.

Note: During the image creation process, Nerdio Manager removes all local user profiles. This increases the likelihood of Sysprep success. Selecting this option bypasses this step. If there are any partially installed APPX apps on the image VM, Sysprep does to remove them.

- **Leave desktop image VM running:** Select this option to leave the VM running after the **Set as image** task completes.

Note: This is useful if you want to push OS and application updates to the running VM.

- **Change log:** Type the list of changes made to the image.
5. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

You can see the job's progress in the logs. See "Desktop Images Change Log Feature" on page 154 for details about the logs.

Desktop Images Scripted Actions

Nerdio Manager enables you to execute scripts on desktop images.

Note: You can execute a scripted action immediately or run it on a schedule.

To execute a scripted action:

1. From the main menu, select **Desktop Images**.
2. From the action menu, select **Run script**.
3. Enter the following information:
 - **Schedule:** Toggle to turn the scheduler **On/Off**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Scripted Actions:** From the drop-down list, select the script you wish to run.

Note:

- Windows scripts are executed via the Azure Custom Script extension and run in the context of the LocalSystem account.
- Azure runbooks are executed via the Azure automation account and run in the context of the Nerdio Manager app service principal.
- The following variables are passed to the script and can be used in the PowerShell commands:
 - \$AzureSubscriptionId
 - \$AzureSubscriptionName
 - \$AzureResourceGroupName
 - \$AzureRegionName
 - \$AzureVMName
 - \$ADUsername (if passing AD credentials)
 - \$ADPassword (if passing AD credentials)
 - \$SATrigger = "RunOnce"
 - \$SATriggerMode = "Manual" | "Schedule"
 - \$DesktopImageVmName
 - \$DesktopImageActiveVersion
 - \$DesktopImageStagedVersion
- **Scripted actions input parameters:** If necessary, provide the required parameters.
- **Pass AD credentials:** Select to pass your AD credentials to the script being executed.
- **Restart VM after script execution:** Select to restart the VM after script execution.

Note: It is preferable to select this option instead of restarting the VM in your PowerShell commands because the Custom Script extension fails if the script restarts the VM.

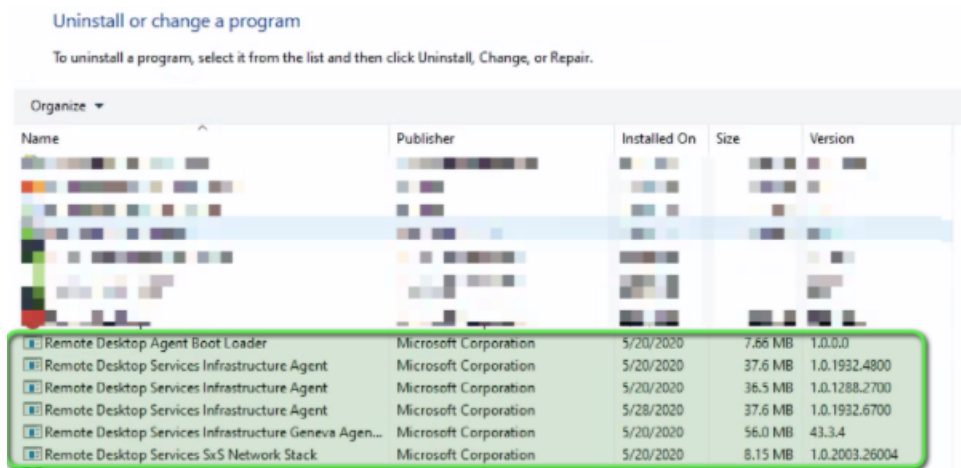
4. Once you have entered all the desired information, select either **Run now** to execute immediately or **Save & close** to save the script and execute as per the schedule.

Desktop Images Manually Uninstall AVD Agent

Before you create a desktop image from an imported VM, you must first manually uninstall the AVD agent.

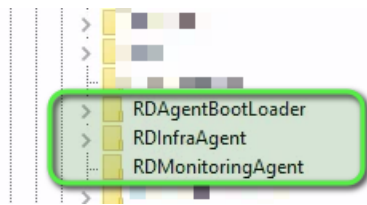
To manually uninstall the AVD Agent:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to work with.
3. Select **Power on**.
4. RDP to the desktop image using the local admin credentials.
5. Navigate to **Control Panel > Programs and Features** and remove all the Remote Desktop programs.



6. In the Registry, navigate to **HKLM\Software\Microsoft**.

7. Remove all traces of the AVD agent (RD*) from the registry, if any.



8. Reboot the desktop and verify that all the components have been removed.
9. In Nerdio Manager, return to **Desktop Images**.
10. Locate the desktop image you just modified and select **Power off and set as image**.

Use Azure to Backup and Restore Desktop Image VM Objects

In Nerdio Manager, you can backup desktop image VM objects to Azure and restore a desktop image VM objects from previous versions. No third-party tools are required, because Nerdio Manager uses the native Azure backup functionality.

When you back up the image VM objects for the first time, it creates all the necessary Azure infrastructure to maintain this backup.

Note: The Microsoft.RecoveryServices Resource Provider must be registered against any Azure subscriptions for which backup is to be enabled. The Nerdio Manager application should then be assigned the Backup Reader role for each subscription where backup should be enabled.

- If the user who configures the backup for the first time is an **Owner** on the subscription, this role is assigned automatically.
- If the user is not an **Owner**, you must manually assign the Backup Reader role to the Nerdio Manager application.

Create a Desktop Image VM Object Backup Policy

Nerdio Manager allows you to create a desktop image VM object backup policy. The policy determines the backup vault, schedule, retention, etc.

Note: A backup policy must be configured in order for manual or automatic backups to be created.

To create a desktop image VM object backup policy:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to back up.
3. From the action down menu, select **Manage backup**.
4. Enter the following information:
 - **Enable Backup:** Toggle on this option.
 - **Vault:** From the drop-down list, select the backup vault.
 - **Policy:** From the drop-down list, select a policy or type the name of a new policy.

Warning: If an existing policy is selected and changed, that changes the policy for all associated devices. It is strongly recommended that you create a new policy for each desktop image.

- **Policy type:** From the drop-down list, select either a Standard or an Enhanced policy type.

Note: Enhanced policies are required to backup Trusted Launch enabled desktops. See this Microsoft [article](#) for details.

- **Schedule:** From the drop-down lists, create the schedule.
 - **Retention:** From the various options, create the retention policy.
5. Once you have entered all the desired information, select **Save**.

Manually Backup a Desktop Image VM Object

Nerdio Manager allows you to manually backup a desktop image VM object to Azure.

To manually backup a desktop image VM object to Azure:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to back up.
3. From the action down menu, select **Backup**.

Note: If a backup policy was not configured for this desktop image, you are prompted to create a backup policy. See "Create a Desktop Image VM Object Backup Policy" on page 147 for details.

4. **Retain image backup:** Type the number of days to retain the backup image.

Note: After the selected number of days, the image backup is automatically deleted. The image VM itself is unaffected when the expired backup version is deleted.

5. Once you have entered all the desired information, select **OK**.

The desktop image VM object is backed up to Azure.

Restore a Desktop Image VM Object from Azure

Nerdio Manager allows you to restore a desktop image VM object from Azure.

To restore a desktop image VM object from Azure:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you want to restore.
3. From the action menu, select **Restore**.
4. From the drop-down list, select the desired recovery point.
5. Select **Restore**.

The desktop image VM object is recovered from the Azure backup vault. By default, this image VM object is powered on.

6. Select **Power off & set as image**.

The VM is committed to the Azure image object from the restored version.

Clone Desktop Images

Nerdio Manager allows you to clone an existing desktop image and create a new one with the same properties. You can create new desktop images based on existing ones and recreate all the customizations associated with your previously created desktop images. There is no need to reconfigure the environment from scratch.

Tip: If you need to replicate your image and move it to another region, simply select a network available in that region as part of the cloning operation. See below for details.

To clone a desktop image:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to clone.
3. From the action menu, select **Clone**.
4. Enter the following information:
 - **Count:** Type the number of image(s) to be created when cloning.
 - **Name:** Type the image's name.
 - **Description:** Type the image's description.
 - **Network:** From the drop-down list, select the network the VM connects to.
 - **VM Size:** From the drop-down list, select the VM size.
 - **OS disk:** From the drop-down list, select the OS disk.
 - **Resource Group:** From the drop-down list, select the resource group.

- **Security type:** From the drop-down list, select the security option that best suits your desktop image VM.

Note:

- **Standard** is set by default. Additional security options are only available for generation 2 VMs with the **Geographic distribution & Azure compute gallery** option enabled.
- The **Trusted launch** and **Confidential virtual machines** security options help improve the security of Azure generation 2 virtual machines. However, additional security features they provide also have some limitations, such as the lack of support for backup, managed disks, and ephemeral OS disks. To learn more, see:
 - [Trusted launch for Azure virtual machines](#)
 - [About Azure confidential VMs](#)

- **Join to AD:** Select this option and from the drop-down list, select the AD.

Note: Unselect this option to not join this desktop image VM to AD during the creation process. This prevents the AD GPOs from applying to the image before it is created. Be sure to specify local administrator credentials below to be able to connect to the VM, since it won't be a member of the AD domain.

- **Skip removal of local profiles:** Select this option to bypass removing all local user profiles.

Note: During the image creation process, Nerdio Manager removes all local user profiles. This increases the likelihood of Sysprep success. Selecting this option bypasses this step. If there are any partially installed APPX apps on the image VM, Sysprep does to remove them.

- **Do not create image object:** Select this option if you do not want to create an image object.
- **Enable time zone redirection:** Select this option if you want users to view the local time zone inside their AVD desktop sessions.
- **Install App Attach certificates:** Select this option if you want to install any stored certificates on the image VM.
- **Set time zone:** From the drop-down list, select the time zone.
- **Optimize disk type when desktop image is stopped:** Select this option to downgrade the OS disk type and save costs. When the machine starts, the OS disk type is changed back to the selected type.
- **Provide custom credentials for a local administrator user:** Toggle this option on if you are the local admin and want to provide the username and password.
- **Geographic distribution & Azure compute gallery:** Toggle this option on if you want to replicate your cloned image across regions.
 - **Azure Compute Gallery:** From the drop-down list, select an existing Azure compute gallery or create a new one.

Note: Only one gallery can be selected. The existing gallery must be in a linked resource group in the same Azure subscription as the image VM.

- **Azure Regions:** From the drop-down list, select the Azure regions where the Desktop Image version should be replicated.

Note: The current Azure region must be part of the selection.

- **Specialized image:** Generalized image is the default option. Select **Specialized image** to create an image that retains all machine and user-specific information. This might be useful if you are creating a VM that is an exact replica of the original machine without resetting or generalizing it.

- **Hibernation supported:** Select this option to deallocate the virtual machine while preserving its memory contents. This allows you to resume the VM from its previous state the next time you start it.

Note: This setting cannot be changed after the VM is created.

- **Stage new image as inactive:** Select this option to create a new image version without activating it. Any existing configurations will continue using the current active version of the image.
 - **Activate staged image after:** Select this option to specify the number of days after which the staged image should be automatically activated. After that period, any linked pools will be updated with the newly activated image.
 - **Current image action:** Select one of the following options:
 - **Remove current version after activation**
 - **Keep current version as backup**
- **Replica Count (Per Region):** Type the number of replicas to allow per region.

Note: The Azure Compute Gallery replicas support a maximum of 20 concurrent clone operations per replica. Ensure that the number of replicas specified meets your deployment requirements. Up to 100 replicas per region are supported. Replicas may only be deployed within the same subscription.

- **Run the following scripted actions before clone image:** Toggle this option on if you want to run scripted actions before cloning the image.
 - From the drop-down list, select the scripted actions.
 - Select **Pass AD credentials** if you want to use them to run the scripted actions.

- **Application Management:** Toggle this option on if you want to manage applications before cloning the image.

Notes:

- You may add as many applications as desired.
 - Drag and drop an application in the list to change its order on the list.
 - Select the "X" next to an application to remove it from the list.
-
- **Install/Uninstall:** Select whether the deployment policy should install or uninstall the selected applications.
 - **Reboot after installation:** Select this option to reboot the cloned image after installation.
 - **Show favorites only:** Select this option to only display applications marked as favorites. Otherwise, you may search the list of applications.
- **Apply tags:** Expand this dropdown to specify the tags to be applied to the image VM, OS disk, network interface, image object, and ACG image.
 - **Tag groups:** Optionally, from the drop-down menu, select the tag groups to assign.

5. Select OK.

The desktop image cloning task begins. It can take up to an hour to complete. You can monitor the progress of the task in the **Desktop Images** tasks section.

Related Topics

- "Import Images from the Azure Library" on page 131
- "Desktop Images Change Log Feature" below

Desktop Images Change Log Feature

In Nerdio Manager you can update, version, or clone desktop images. The desktop images are updated frequently by different users so over time it gets difficult to track changes made to them.

It is important to track these changes as desktop images are the foundation of AVD host pools.

The Nerdio Manager Change Log feature helps admins keep track of all changes made to desktop images.

To set up a change log for a desktop image:

1. Navigate to **Desktop Images**.
2. Select a desktop image that you wish to maintain a change log for.
3. Select the **Power off & set as Image**.

The **Set as an Image** window opens.

4. Type the list of changes made to the image in the **Change log** section.
5. Select **Run now**.

The change log record is attached to the desktop image.

You can view all changes that were done manually or automatically to the desktop image

To view the change log for a desktop image:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you wish to view.
3. From the action menu, select **Change Log**.

The changed image details are displayed.

Related Topics

"Import Images from the Azure Library" on page 131

"Import an Existing VM" on page 137

"Clone Desktop Images" on page 150

Refresh Desktop Images from the Azure Marketplace

Nerdio Manager allows you to refresh desktop images from the Microsoft published and managed images in the Azure marketplace.

This automated image refresh operation ensures that you always have a pristine image from Microsoft with all the latest OS patches applied. The refreshed image is automatically deployed to all session hosts that use it.

To refresh a desktop image from the Azure Marketplace:

1. Navigate to **Desktop Images**.
2. Locate the image you want to refresh.
3. Select the **Power off & Set as image**.
4. In the **Schedule** section, enable the scheduling function.
5. Enable **Refresh image from Azure Marketplace**.
6. Enter the following information:

- **Marketplace Image:** From the drop-down list, select an image.
- **Join to AD:** Select this option and then from the drop-down list, select an Entra Domain Services or an AD profile to directly join the image.

For example, you can select a Windows 10 (2004) EVD _ Office ProPlus -Gen2 (multi-session) image and join it to the nerdio.int (default) AD. You can schedule to refresh this image, weekly, starting 11/20/2021 at 12:00 every Saturday

You can run scripted actions (for example, installing Microsoft Teams, Zoom client, etc.) along with the image refresh.

7. Select **Run now** (not scheduled) or **Save & close** (scheduled).

Related Topics

"Import an Existing VM" on page 137

"Desktop Images Change Log Feature" on page 154

Stage Desktop Images

To allow administrators to test and validate changes to an image before deploying to the wider user base, Nerdio Manager provides an Image Staging feature that allows Nerdio Manager to deploy images to a test or "Staging" pool before activation.

Note: This option is available only for desktop images that have been recently refreshed from the Azure Marketplace. This option is usually preferred by highly compliant environments. For more information about refreshing images from the Azure Marketplace refer to "Refresh Desktop Images from the Azure Marketplace" on the previous page.

Enable Desktop Image Staging

The following steps allow you to enable staging for a desktop image.

To enable desktop image staging:

1. Navigate to **Desktop Images**.
2. Locate the image you wish to work with.
3. From the action menu, select **Set as image** or **Power off & set as image** (according to the power state of the desktop image).
4. Enter the following information:
 - **Geographic distribution & Azure compute gallery:** If not already **On**, toggle **On** this option and select the following:
 - **Azure Compute Gallery:** From the drop-down list, select an existing Azure Compute Gallery or create a new one.
 - **Azure Regions:** From the drop-down list, select Azure regions where the Desktop Image version should be replicated.
 - **Stage new image as inactive:** Select this option to create the new image version without setting it as active.

Notes:

- Any existing configurations continue using the current version of the image. To make the new version active, see "Deploy an Inactive Staged Desktop Image" on the next page for details.
- By default, the option **Save current image as a backup** is not selected. If you select this option, a new image is created, but Nerdio Manager keeps it as inactive with an older version number.

- **Activate staged image after:** Optionally, select this option to automatically activate the staged image after the specified number of days.

Note: Any pools linked pools have their associated image updated.

- **Current version action:** From the drop-down list, select the action for the current version.

Note: Select the **Keep current version as backup** option to retain the current image version as a standalone object. This image version is not visible or manageable via Nerdio Manager, so be sure to delete it manually when no longer needed to avoid unnecessary Azure storage costs. Prior versions of ACG images can be utilized under **Unmanaged ACG image versions** in the Desktop Image (template) menu.

5. Once you have entered all the desired information, select **Run now**.

The "Power off & set as desktop image" task is triggered.

You can view the status of the task in the **Desktop Images Tasks** section.

DESKTOP IMAGES TASKS						
TASK	RESOURCE NAME	USER	STATUS	CREATED	COMPLETED	
Power off & set as image	GovimgTest	spatwardhan@getnerdio.com	COMPLETE	Nov 15, 2021 08:54 PM	Nov 15, 2021 09:14 PM	Details Hide

6. Wait for the task to finish. The two images are now in the list.

Edit Desktop Image Staging Auto-activation Settings

The following steps allow you to edit the auto-activation settings of a staged desktop image.

To edit desktop image staging auto-activation:

1. Navigate to **Desktop Images**.
2. Locate the image you wish to work with.
3. From the action menu, select **Configure auto-activation**.
4. Enter the following information:
 - **Activate staged image after:** Optionally, select this option to automatically activate the staged image after the specified number of days.

Note: Any pools linked pools have their associated image updated.

- **Current version action:** From the drop-down list, select the action for the current version.

Note: Select the **Keep current version as backup** option to retain the current image version as a standalone object. This image version is not visible or manageable via Nerdio Manager, so be sure to delete it manually when no longer needed to avoid unnecessary Azure storage costs. Prior versions of ACG images can be utilized under **Unmanaged ACG image versions** in the Desktop Image (template) menu.

5. Once you have entered all the desired information, select **Save & close**.

Deploy an Inactive Staged Desktop Image

The following steps allow you deploy an inactive staged desktop image.

To deploy an image that is inactive:

1. Navigate to **Desktop Images**.
2. Select the inactive image you want to deploy.
3. From the action menu, select **Activate staged image**.
4. Select **Save current image version as a backup**.
5. Select **OK**.

The staging image becomes the active version. The older version is saved as backup and is no longer be shown in the list.

Related Topics

"Refresh Desktop Images from the Azure Marketplace" on page 156

FSLogix and User Profile Management

FSLogix is a user profile container technology (FSLogix Profile Containers) that allows users to switch virtual desktops session host without losing access to their own customizations. With FSLogix, you can use OneDrive and the indexed search functionality in virtual desktops. This option was not available for the legacy RDS User Profile Disks (UPDs).

FSLogix is integrated with AVD and provides, by default, an on-demand seamless user profile storage solution. The AVD for Business and SharePoint functionality level matches that of a stationary desktop, for example, on a physical PC or a laptop.

FSLogix supports active cache syncing in the AVD environment so that users get their updated files from any of the connected hosts.

FSLogix retains the user credentials. You do not need to sign in to OneDrive every time you start a session.

The Windows user profiles of AVD desktop users are encapsulated in VHD files and stored on a file server separate from the session host VMs. If a user is assigned to a pooled (for example, non-persistent) desktop, the profile including Windows Search cache follows the user regardless of the virtual desktop VM they sign in to.

Nerdio Manager makes sure that setting up, configuring, and managing FSLogix Profile Containers is easy to do. Multiple so-called FSLogix configuration profiles can be created, which can be applied per host pool. This means you can have different FSLogix configurations where, for example, the storage locations are different (often in the form of Azure Files, see "Create and manage configured Azure Files shares" on page 347 for more information) or where you have different registry parameters set, again, on a per-host pool level.

We ensure that the proper agent is installed on your image, or explain how to do it manually, and that the correct configuration profile is applied. Meaning, that when a session host VM is joined to the host pool, or is re-imaged, all of this is automatically taken care of.

Related Topics

"FSLogix settings and configuration" on the next page

FSLogix settings and configuration

The FSLogix profile container is based on two components:

- Installation of the FSLogix application (https://aka.ms/fslogix_download)
- Configuration of the FSLogix via GPO or registry. For more information, see this [Microsoft article](#).

Nerdio Manager automatically installs the FSLogix application, by default, when a new session host VM is created, or an existing one is re-imaged. This is the most common use case.

Create an FSLogix profiles storage configuration

Nerdio Manager allows you to create FSLogix Profiles storage configurations.

To add an FSLogix Profiles storage configuration:

1. Navigate to **Settings > Integrations**.
2. In the **FSLogix Profiles storage** tile, select **Add**.
3. Enter the following information:
 - **Name:** Type the profile name.
 - **Version** From the drop-down list, select the FSLogix version.
 - **Use Cloud Cache:** Select this option to enable FSLogix Cloud Cache.

Tip: For performance reasons, it is strongly recommended that you use Premium SSD and Ephemeral OS disks when Cloud Cache is enabled. (Standard SSD disks might be sufficient in very small environments or a testing scenarios.)

Note: See the following Microsoft [article](#) for more information about FSLogix Cloud Cache.

Cloud Cache allows you to specify multiple profile storage location. It asynchronously replicates the profiles and makes the profiles available in multiple storage locations at the same time. So, if one of the locations is not available, the session host automatically fails over to one of the alternate locations.

- **Use Azure Page Blobs:** If Cloud Cache is enabled, select this option to use storage account blob containers to store user profiles. These containers are accessed using storage account access keys.
- **Configure session hosts registry for Entra ID joined storage:** Select this option to enable Entra ID Kerberos functionality and Entra ID account credentials loading.

Note: See this Microsoft [article](#) for more information.

- **Exclude the local admin accounts from FSLogix:** Select this option to prevent local admins profiles creation in FSLogix storage location.

Note: When FSLogix is having issues on a session host, there is still a way to sign in with an excluded user for troubleshooting purposes.

- **Manage App Service settings:** Select this option to to edit the FSLogix App Service Registry settings.

Manage App Service settings ⓘ

App Service Settings ⓘ

SETTING NAME	CONFIGURATION	DEFAULT
CleanupInvalidSessions ⓘ	Not configured ⓘ	0
RoamRecycleBin ⓘ	Not configured ⓘ	1
VHDCompactDisk ⓘ	Not configured ⓘ	1

- **Manage Log settings:** Select this option to manage log settings.

SETTING NAME	CONFIGURATION	DEFAULT
LogDir ⓘ	Not configured	%ProgramData%\FSLogix\ Logs
LogFileKeepingPeriod ⓘ	Not configured ⓘ	2
LoggingEnabled ⓘ	Not configured ⓘ	2
LoggingLevel ⓘ	Not configured ⓘ	1

- **FSLogix Profiles path (CCDLocation):** From the drop-down list, select an Azure Files share. Alternatively, type in a UNC path.
 - Optionally, select **Override** to override the default storage path.

Note: You can specify up to 4 paths. In addition, use the arrows to change the order of the paths. The profiles are created in all of these locations.

- **FSLogix Registry Options:** From the drop-down list, select whether you want to work with **All settings** or **Advanced**.
 - For **All settings**:

Clear all

SETTING NAME	CONFIGURATION	DEFAULT
AccessNetworkAsComputerObject ⓘ	Not configured ⓘ	0
AttachVHDSDDL ⓘ	Not configured	
CleanOutNotifications ⓘ	0 ⓘ	Clear
DeleteLocalProfileWhenVHDSshouldApply ⓘ	Not configured ⓘ	0
DiffDiskParentFolderPath ⓘ	Not configured	%TEMP%
FlipFlopProfileDirectoryName ⓘ	Not configured ⓘ	0
IgnoreNonWWD ⓘ	Not configured ⓘ	0

- In the **Configuration** column, type the setting's value.
- Select **Clear** to set a specific setting to **Not configured**.

- Select **Clear all** to set all the settings to **Not configured**.
- For **Advanced**:
 - You can add DWORD values in the format:
`"ValueName":dword:ValueData` (example:
`"ProfileType"=dword:00000003`).
 - You can add string values in the format: `"ValueName":"ValueData"`
(example: `"VolumeType":"vhdx"`).
- **Configure Office Container to redirect Microsoft Office user data**: Toggle on this option to redirect only areas of the profile that are specific to Microsoft Office.

Note: Office Containers separate Microsoft Office data (for example, OST files) from the overall user profile for easier troubleshooting. Office Containers and Profile Containers are stored in separate VHDX files can be stored on different file shares. See this Microsoft [article](#) for details.

- **FSLogix Office Container path (VHDLocation)**: Modify as needed.
- **FSLogix Office Container Registry Options**: Modify as needed.
- **Redirections**: Select this option if you want to include Redirections in the global profile for re-use across customers.

Note: See this Microsoft [article](#) for more information about redirections.

- **Force the installation of FSLogix apps even if already installed**: Select this option to force the re-installation of the FSLogix agent and applications.
4. Once you have entered all the desired information, select **OK**.

Set an FSLogix profiles storage configuration as default

Nerdio Manager allows you to set one FSLogix Profiles storage configuration as the default.

To set Nerdio Manager to install the FSLogix application automatically:

1. Navigate to **Settings > Integrations**.
2. In the **FSLogix Profiles storage** tile, add, change, and remove the profiles as needed.

Notes: Be sure to select the following options for FSLogix profiles linked to hybrid host pools.

- **Use Cloud Cache:** Select this option to enable FSLogix Cloud Cache in the host pools, and the session hosts within those host pools, that use this FSLogix profile.
- **Use Azure page blobs:** Select this option to use storage account blob containers to store users profiles. These containers are accessed using storage account access keys.

3. Locate the desired FSLogix Storage configuration profile and select **set default**.

Notes:

- If you set the **Use FSLogix Profiles** option to **Off**, the FSLogix app is installed automatically when new hosts are created or re-imaged.
- Each host pool's FSLogix settings can be customized.
- FSLogix is not installed on the desktop image.
- The FSLogix registry settings are not set on the desktop image.
- Session hosts should not receive conflicting FSLogix configurations from GPOs.

Related Topics

"FSLogix and User Profile Management" on page 161

"FSLogix Per-Host Pool Customization" below

FSLogix Per-Host Pool Customization

You can configure FSLogix with Nerdio Manager and apply its settings to each host pool in the AVD deployment.

For more information refer to "Host Pools" on page 204.

Adding a server includes installing FSLogix and applying the necessary settings that were selected for the host pool. You can use the global default settings or customize the settings for each host pool.

To configure customized FSLogix settings for a host pool:

Note: Any settings configured here are applied only to newly created or re-imaged hosts in this pool.

1. Navigate to the list of host pools and locate the host pool you wish to change.
2. From the action menu, select **Properties > FSLogix**.
3. Enter the following information:
 - Toggle **Use FSLogix profiles** to **On**.

Note: If this option is not enabled, Nerdio Manager does not install the FSLogix profile container application on newly created VMs when they are deployed in this host pool. Existing VMs are not affected.

- **Profile:** From the drop-down list, select an existing profile name. Alternatively, select **Custom** to create a custom profile for this host pool.
- **Version** From the drop-down list, select the FSLogix version.
- **Use Cloud Cache:** Select this option to enable FSLogix Cloud Cache.

Tip: For performance reasons, it is strongly recommended that you use Premium SSD and Ephemeral OS disks when Cloud Cache is enabled. (Standard SSD disks might be sufficient in very small environments or a testing scenarios.)

Note: See the following Microsoft [article](#) for more information about FSLogix Cloud Cache.

Cloud Cache allows you to specify multiple profile storage location. It asynchronously replicates the profiles and makes the profiles available in multiple storage locations at the same time. So, if one of the locations is not available, the session host automatically fails over to one of the alternate locations.

- **Use Azure Page Blobs:** If Cloud Cache is enabled, select this option to use storage account blob containers to store user profiles. These containers are accessed using storage account access keys.
- **Configure session hosts registry for Entra ID joined storage:** Select this option to enable Entra ID Kerberos functionality and Entra ID account credentials loading.

Note: See this Microsoft [article](#) for more information.

- **Exclude the local admin accounts from FSLogix:** Select this option to prevent local admins profiles creation in FSLogix storage location.

Note: When FSLogix is having issues on a session host, there is still a way to sign in with an excluded user for troubleshooting purposes.

- **Manage App Service settings:** Select this option to to edit the FSLogix App Service Registry settings.

Manage App Service settings ⓘ

App Service Settings ⓘ

SETTING NAME	CONFIGURATION	DEFAULT
CleanupInvalidSessions ⓘ	Not configured ⓘ	0
RoamRecycleBin ⓘ	Not configured ⓘ	1
VHDCompactDisk ⓘ	Not configured ⓘ	1

- **Manage Log settings:** Select this option to manage log settings.

SETTING NAME	CONFIGURATION	DEFAULT
LogDir ⓘ	Not configured	%ProgramData%\FSLogix\ Logs
LogFileKeepingPeriod ⓘ	Not configured ⓘ	2
LoggingEnabled ⓘ	Not configured ⓘ	2
LoggingLevel ⓘ	Not configured ⓘ	1

- **FSLogix Profiles path (CCDLocation):** From the drop-down list, select an Azure Files share. Alternatively, type in a UNC path.

Note: You can specify up to 4 paths. In addition, use the arrows to change the order of the paths. The profiles are created in all of these locations.

- **FSLogix Registry Options:** From the drop-down list, select whether you want to work with **All settings** or **Advanced**.
 - For **All settings**:

[Clear all](#)

SETTING NAME	CONFIGURATION	DEFAULT
AccessNetworkAsComputerObject ⓘ	Not configured ⓘ	0
AttachVHDSDDL ⓘ	Not configured	
CleanOutNotifications ⓘ	0 ⓘ	Clear
DeleteLocalProfileWhenVHDSshouldApply ⓘ	Not configured ⓘ	0
DiffDiskParentFolderPath ⓘ	Not configured	%TEMP%
FlipFlopProfileDirectoryName ⓘ	Not configured ⓘ	0
IgnoreNonWVD ⓘ	Not configured ⓘ	0

- In the **Configuration** column, type the setting's value.
- Select **Clear** to set a specific setting to **Not configured**.
- Select **Clear all** to set all the settings to **Not configured**.

- For **Advanced**:
 - You can add DWORD values in the format:
`"ValueName":dword:ValueData` (example:
`"ProfileType"=dword:00000003`).
 - You can add string values in the format: `"ValueName":"ValueData"`
(example: `"VolumeType":"vhdx"`).
- **Configure Office Container to redirect Microsoft Office user data**: Toggle on this option to redirect only areas of the profile that are specific to Microsoft Office.

Note: Office Containers separate Microsoft Office data (for example, OST files) from the overall user profile for easier troubleshooting. Office Containers and Profile Containers are stored in separate VHDX files can be stored on different file shares. See this Microsoft [article](#) for details.

- **FSLogix Office Container path (VHDLocation)**: Modify as needed.
- **FSLogix Office Container Registry Options**: Modify as needed.
- **Redirections**: Select this option if you want to include Redirections in the global profile for re-use across customers.

Note: See this Microsoft [article](#) for more information about redirections.

- **Force the installation of FSLogix apps even if already installed**: Select this option to force the reinstallation of the FSLogix agent and applications.
- **Apply to existing hosts**: Select this option to apply these changes to existing hosts. Otherwise, the change only effect new or re-imaged hosts.
 - **Process hosts in groups of**: Type the number of concurrent actions to execute during this bulk operation.
 - **Number of failures before aborting**: Type the number of failures that causes the process to stop.

- **Messaging:** Toggle on the Messaging to send messages to active users.
 - **Delay:** From the drop-down list, select the number of minutes to wait after sending the message before starting the process.
 - **Message:** Type the message you want to send to the users.
- **Schedule:** Toggle on the Schedule to apply the changes at a selected time.
 - **Start Date:** Type the date to start.
 - **Time Zone:** From the drop-down list, select the time zone for the Start time.
 - **Start Time:** From the drop-down lists, select the time to start.
 - **Repeat:** From the drop-down list, select the recurring schedule, if desired.

Note: The drop-down has the option **After Patch Tuesday**. This allows you to create a recurring schedule based on [Patch Tuesday](#).

- **Days After:** If you selected **After Patch Tuesday**, type the number of days after Patch Tuesday to run the scheduled task.

4. Once you have entered all the desired information, select **Save** or **Save & close**.

Related topics

"Host Pools" on page 204

Host Pool Disaster Recovery: You can enable host pool level active/active DR configuration and Nerdio Manager automatically distributes session hosts across two Azure regions. Users are distributed across VMs in both regions as they sign in and FSLogix profiles are automatically replicated using Cloud Cache. In case of an Azure region failure users continue to access VMs in the available region. See this [demo](#) for more information.

FSLogix Shrink VHD/VHDX Containers (Scripted Action)

Nerdio Manager has a powerful automation that enables you to save money on FSLogix storage capacity by shrinking the white space inside of FSLogix's VHD/VHDX containers.

As data is added to the VHD/VHDX file, it grows. If the data is later removed, the VHD/VHDX file has more free space but the size of the file does not decrease. This is capacity that you are consuming and paying for but is not utilized.

Nerdio Manager has an Azure runbook scripted action that can take these VHD files in bulk, discover the white space inside them, and shrink them.

To shrink the FSLogix VHD/VHDX containers using a scripted action:

1. Create the following Global Secure Variables: (See "Scripted Actions Global Secure Variables" on page 189 for details.)
 - **FslResourceGroup**: The resource group in which the temp VM is created.
 - **FslTempVmVnet**: The VNet in which the temp VM is created.
 - **FslTempVmSubnet**: The subnet in which the temp VM is created.
 - **FslStorageUser**: The storage account key user or AD user with access to the fileshare.
 - **FslStorageKey**: The storage account key or AD password.
 - **FslFileshare**: The UNC path to the FSLogix profiles share.
2. Navigate to **Scripted Actions > Azure runbooks**.
3. Locate the script called **Shrink FSLogix Profiles**.
4. From the action menu, select **Run now** or **Schedule**.

Scripted Actions Overview

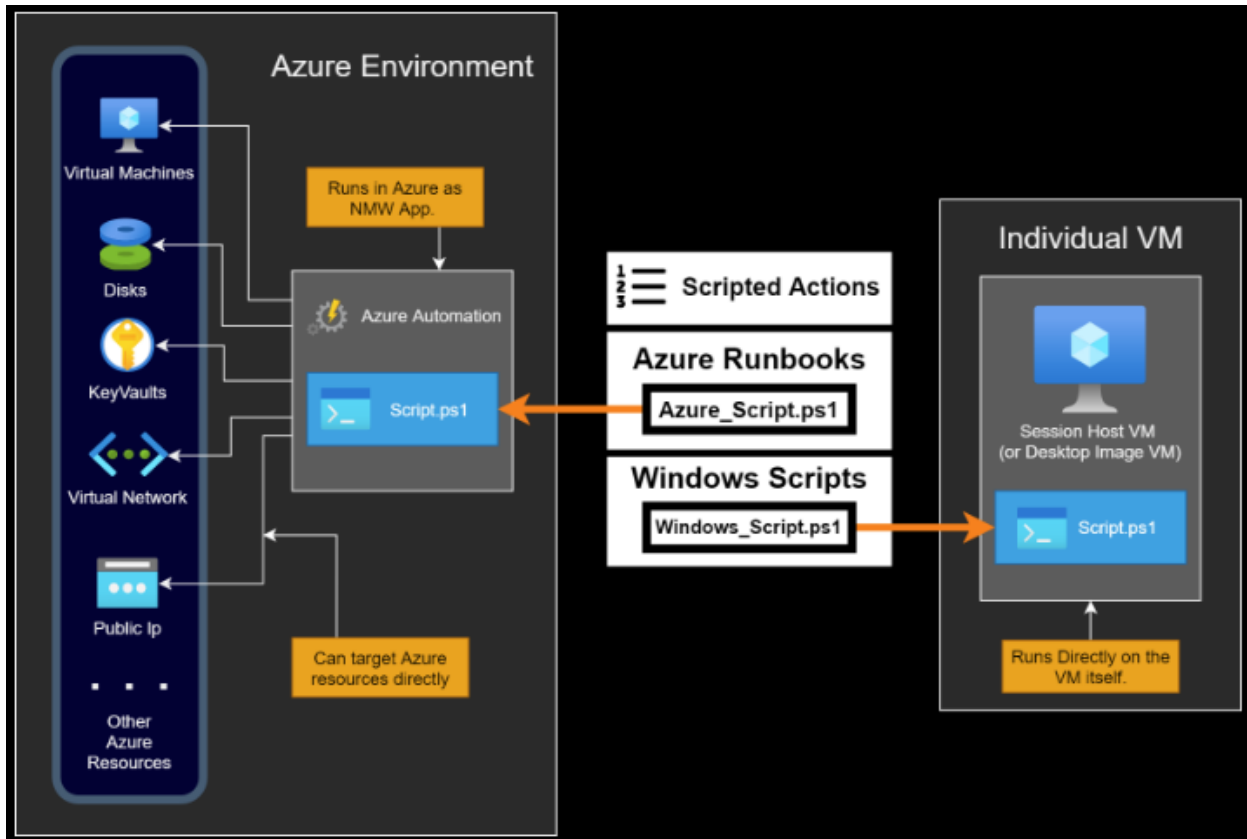
Scripted Actions are PowerShell scripts that run either in the context of a Windows VM or an Azure Automation Account. Scripted Actions can be used to extend and customize the functionality of Nerdio Manager. Nerdio Manager provides several pre-populated variables, such as `$VMName`, that can be used in the PowerShell code.

Nerdio Manager contains many out-of-the box scripted actions. In addition, scripts can be created and customized by the Nerdio Manager administrators. They can be applied at various stages of the Nerdio Manager automation. For example, when a Virtual Machine is created, shut down, or removed. You can apply an action on a schedule, or to desktop images, and more.

Nerdio Manager uses two types of scripted actions:

- Windows scripts - "Scripted Actions for Windows Scripts" on page 194
- Azure runbooks - "Scripted Actions for Azure Runbooks" on page 197

Scripted Actions serve as a library of PowerShell scripts that can be run in either Azure or AVD Virtual Machines, as an included step for various tasks performed by Nerdio Manager.



Create a New Scripted Action

To create a new scripted action:

1. Navigate to **Scripted Actions**.
2. Select either **Windows scripts** or **Azure runbooks**.
3. Select **Add scripted action**.
4. Enter the following information:
 - **Name:** Type the name of the script. This name is displayed when you select this action from the list of available scripted actions.
 - **Description:** Type the script's description.

- **Tags:** From the drop-down list, select optional tags for the script. These tags are used for searching and organization.
- **Script Execution Mode:** From the drop-down list, select the script's execution mode.

Note: This parameter determines how Nerdio Manager acts when it passes the scripted action(s) to the VM. Nerdio Manager uses the Azure Custom Script Extension to ultimately execute the PowerShell commands (for more information about Scripted Actions for windows refer to [Custom Script for Windows](#)). The extension needs to be installed and removed every time Nerdio Manager executes a Windows Scripted Action. Optionally, PowerShell scripts can be combined and passed in a single run, if they do not interfere with each other, thus saving time.

- **Combined:** Marks the script as one that can be combined safely with other scripts. For example, a script that adds a registry value.
- **Individual:** A stand-alone script for an action that should be run on its own. For example, a long script with commonly used variable names that may conflict with other scripts, or a script that requires a fresh PowerShell session.
- **Individual with restart:** For Windows scripts, run the script in stand-alone mode and perform a restart when complete.
- **Execution Timeout:** For Azure runbooks in Individual mode, type the timeout (in minutes) for the scripted action execution.
- **Enable Cloud PC:** Optionally for Windows scripts, toggle this option on to create a Cloud PC script policy.
 - **Run this script using the logged on credentials:** Select this option to run the script with the user's credentials on the client computer. By default, the script runs in system context.
 - **Enforce script signature check:** Select this option to enforce that the script must be signed by a trusted publisher. By default, no warning or prompt displays and the script runs unblocked.

- **Run script in 64 bit PowerShell Host:** Select this option to run the script in a 64-bit PowerShell Host for a 64-bit client architecture.
 - **Assign to all users:** Select this option to assign the script to all users.
 - **Assign to all devices:** Select this option to assign the script to all devices.
 - **Assign to selected groups:** From the drop-down list, select the group(s) to assign this script to.
 - **Exclude assignments:** From the drop-down list, select the group(s) to exclude this script from.
- **Script:** Type the PowerShell command(s) to execute.

Note: Nerdio Manager allows you to integrate variables into the Azure runbooks scripted actions. See "Scripted Actions: Azure runbooks variables integration" on page 187 for more information.

Note: Cmdlets used in this code must be available on the VMs or in the Azure Automation account. If using PowerShell cmdlets from modules not present by default on the Windows VMs or in the Azure Automation account, the modules must first be installed.

Nerdio provides several pre-populated variables that can be used in the script code. The available variables are:

- \$HostPoolId (Available when the script is associated with a host pool)
- \$HostPoolName (Available when the script is associated with a host pool)
- \$AzureSubscriptionId
- \$AzureSubscriptionName
- \$AzureResourceGroupName
- \$AzureRegionName
- \$AzureVMName (Available when the script is associated with a VM)
- \$ADUsername (if passing AD credentials)
- \$ADPassword (if passing AD credentials)
- \$DesktopUser (Available when the script is associated with a personal host pool)

Tip: It is recommended to develop code using an IDE such as VSCode or ISE. Then test the PowerShell code on a dedicated development session Host /Azure VM.

5. Once you have entered all the desired information, select **Save & close**.

View and Edit Existing Scripted Actions

Nerdio Manager allows you to view or edit existing scripted actions.

To view and edit an existing scripted action:

1. Navigate to **Scripted actions**.
2. Select either **Windows Scripts** or **Azure runbooks**.
3. Locate the scripted action you want to work with and select **Edit**.
4. If desired, make the necessary changes and select **Save** and **close**.

Clone a Scripted Action

Nerdio Manager allows you to clone a scripted action.

To clone a scripted action:

1. Navigate to **Scripted actions**.
2. Select either **Windows Scripts** or **Azure runbooks**.
3. Locate the scripted action you want to clone, and from the action menu select **Clone**.
4. Make all the necessary changes and select **Clone**.

Scripted Actions Groups

Scripted Actions Groups allows administrators to create script collections and assigns these during standard deployment tasks. See "Scripted Actions Groups" on page 181 for details.

Apply Scripted Actions

Scripted Actions can be used as part of these tasks:

- **VM Lifecycle Events:** Executed during the provisioning or re-imaging of Session Host VMs, or when a VM is stopped/started. Whenever a session host is created, destroyed, stopped, or started, the scripted action is performed as a final step. For more information about re-imaging the hosts refer to "Resize/Re-image a Host Pool" on page 270.
- **Run Script:** Manually run a command against a host pool. This is useful if you need to change all the session hosts without fully re-imaging them (for example, a script to change a registry key). For more information refer to "Run Bulk Host Scripted Actions" on page 287.

To apply a configured scripted action to AVD host VM lifecycle events:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > VM Deployment**.
3. Toggle on the desired **Run scripted actions when...** options.
4. For each option, enter the following information:
 - **Script:** From the drop-down list, select the script to execute.
 - **Scripted actions input parameters:** If necessary, provide the required parameters.
 - **Pass AD credentials:** Select this option to pass AD credentials to the script as variables.
 - **AD Credentials:** From the drop-down list, select the AD credentials to pass.
5. Once you have entered all the desired information, select **Save & close**.

The scripted actions are added to the list of scripted actions for this host pool.

Warning: For some automations, the necessary actions to take must be done in the context of Azure, outside of the VM itself. While these commands could be run on the session host VM with the Azure PowerShell module installed, running scripts on session hosts that target Azure are less efficient and can be unreliable. Azure Automation allows for consistent execution, and allows for the Nerdio Manager to run the scripts as itself easily. Some scripts even require the VM to be restarted or shutdown, which means it could not be run on the session host VM regardless.

For information about troubleshooting the Azure scripts, refer to "Troubleshoot Scripts" on page 190.

To run a scripted action on the Host Pool using the Run Script option:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Hosts > Run script**.
3. Enter the following information:

- **Run the following scripted actions on all VMs in ...:** From the drop-down list, select the scripted actions that you want to apply.
- **Scripted actions input parameters:** If necessary, provide the required parameters.
- **Pass AD credentials:** Select this option to pass AD credentials.
- **AD Credentials:** From the drop-down list, select the AD credentials to pass.
- **Restart VMs after scripted action:** Select this option to restart the VMs after script execution. It is preferable to use this option instead of using any PowerShell restart commands as Custom Script extension fails if the script restarts the computer.
- **Process hosts in groups of:** Type the number of concurrent actions to execute during this bulk operation
- **Number of failures before aborting:** Type the number of failures that causes the process to stop.
- **Schedule:** Toggle on the Schedule, and enter the schedule information, to enable running the script per a schedule.
- **Messaging:** Toggle on the Messaging to send messages to active users.
 - **Delay:** From the drop-down list, select the number of minutes to wait after sending the message before starting the process.
 - **Message:** Type the message you want to send to the users.

4. Once you have entered all the desired information, select **Save & close**.

Related Topics

"Resize/Re-image a Host Pool" on page 270

"Run Bulk Host Scripted Actions" on page 287

"Scripted Actions for Windows Scripts" on page 194

"Scripted Actions for Azure Runbooks" on page 197

"Troubleshoot Scripts" on page 190

Scripted Actions Groups

Scripted Actions Groups allows administrators to create script collections and assign them during standard deployment tasks.

Scripted actions group tasks are not performed in isolation. If a scripted action group is deployed as part of task, it operates in exactly the same way as it would if the scripts had been added individually. Therefore, administrators should ensure that tasks within a scripted actions group are ordered correctly for the required outcome. In addition, ensure that the order of both individual scripted actions and scripted actions groups within the task are sequenced appropriately.

To create a scripted actions group:

1. Navigate to **Scripted Actions > Scripted actions groups**.
 2. Select **Add scripted actions group**.
 3. Enter the following information:
 - **Name:** Type the name of the scripted actions group. This name is displayed when you select this action from the list of available scripted actions.
 - **Description:** Type the group's description.
 - **Tags:** From the drop-down list, select optional tags for the group. These tags are used for searching and organization.
 - **Scripted Actions:** From the drop-down list, select the scripted action(s) to include in the group.
- Note:** The scripted actions are performed in the order specified in the list. You can drag & drop a script to change its order in the list.
- **Default parameters:** If necessary, provide the default parameters.
 4. Once you have entered all the desired information, select **Save & close**.

Note: The new scripted actions group is now available for deployment tasks. See "Scripted Actions Overview" on page 173 for details.

Default Scripts for Nerdio Manager

Every installation of Nerdio Manager contains default scripted actions. These are commonly used scripts and examples that you can use or reference for your own scripts. Default scripts have the Nerdio Tag and are locked for editing. You can clone them in order to create a customized, editable version.

Note: This is a partial list. Nerdio continuously updates the default Scripted Actions.

Default Window Scripts

Name	Use Case	Recommended Target	Requires Customization*
Install MS Teams	Save time manually uninstalling and reinstalling MS Teams. Also enables AVD Mode.	Image VMs (preferred), Session Hosts	No
Install MS 365 Office Apps	Save time manually updating MS Office apps.	Image VMs	Yes: If the default list of apps installed is not desired.
Virtual Desktop Optimization	Optimize session hosts for better performance. Commonly used for Remote App Session hosts.	Session Hosts	Yes: By default, many apps are removed, such as calculator. If this is not desired, remove them from the script.
Install Zoom VDI Client	Installs Zoom (VDI Version).	Image VMs	No

Name	Use Case	Recommended Target	Requires Customization*
Enable RDP Shortpath	Enables RDP Shortpath	Image VMs or Session Hosts	No
Enable AVD Screen Capture Protection	Enables screen capture protection. Note: This is an example of how to use PowerShell to edit registry via scripted actions.	Image VMs or Session Hosts	No
Grant user local admin rights	Adds user who is assigned to the personal desktop VM to the local admin group.	Session Hosts	No
Update Windows	Runs Windows 10/11 Updates.	Image VMs	No

*This script is intended to be cloned and edited to suit your needs.

Default Azure Runbooks

Name	Purpose	Requires Customization*
Assign Public IP to VM	Allows VM to have a public IP.	Yes: If Static IPs are required or naming scheme is not desired.
Enable Anti-Malware Extension	Adds anti-malware extension.	Yes: If custom exclusions or scan settings times are needed.
Enable VM OS Disk Encryption	Encrypts Disk with Key Vault.	Yes: If using an existing key vault.

*This script is intended to be cloned and edited to suit your needs.

Considerations for Scripted Actions

Considerations for Window Scripted Actions

For information about Windows scripted actions considerations refer to [Custom Script Windows - Tips and Tricks](#).

- Custom script extensions have a 90-minute timeout set by Azure. The script fails after 90 minutes if:
 - It is stuck.
 - It waited too long for user input.
 - It did not complete on time.
- The script is run with administrative privileges and does not interrupt other sessions. Most scripts are safe to run while users are on the VM.

Note: For information about troubleshooting Windows scripts refer to "Troubleshoot Scripts" on page 190.

Considerations for Azure Scripted Actions

Some general conventions and common procedures used for runbooks are not applicable in Nerdio Manager.

These key considerations are important:

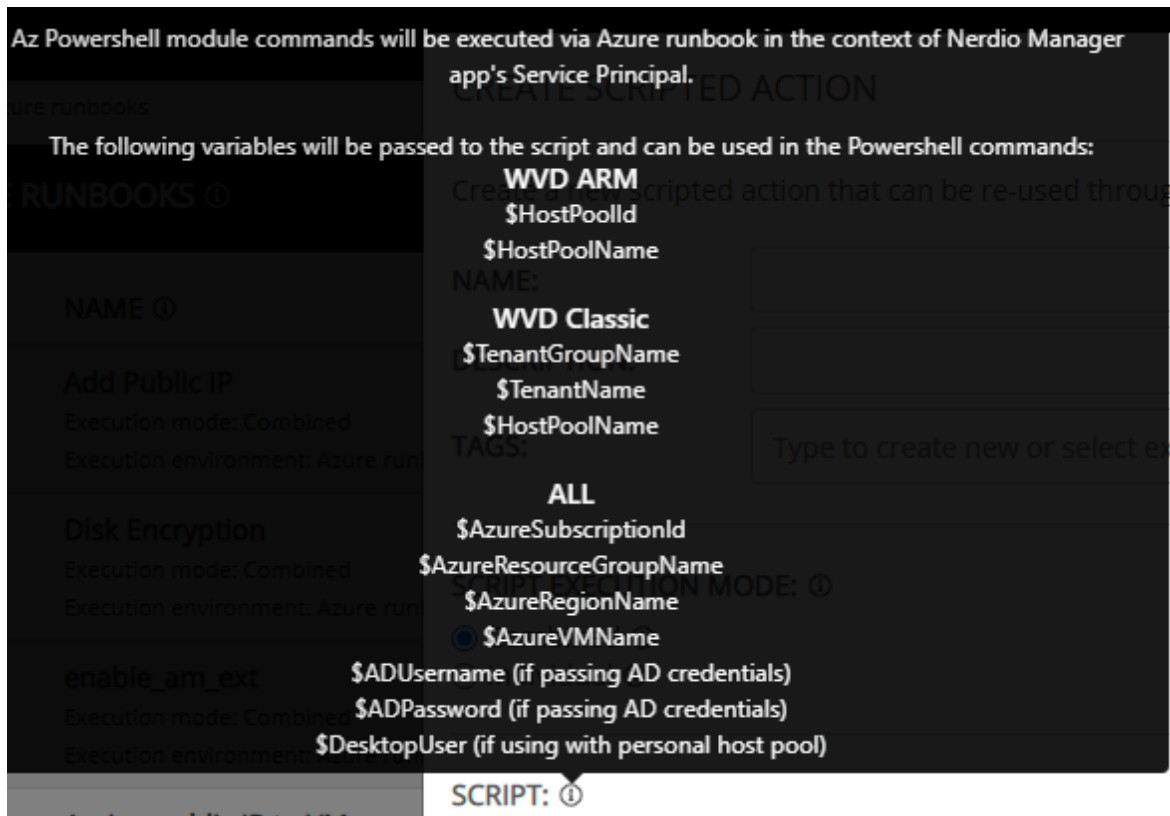
- There is no need to specify authentication, such as authenticating using the RunAs account or passing a credential. By the time the actual code in the scripted action is executed, Nerdio Manager is already logged in to Azure, and no additional authentication is required.

Note: In this case, the Nerdio Manager service principal needs the appropriate permissions on resources it attempts to alter.

- Azure Modules are already installed in the Azure Automation Account. If you require a specific version, change the modules attached to the automation account. Any other modules that are needed require additional installation.
- Some Variables are defined prior to your code. This is useful to get the necessary parameters. For example, the VM name, the subscription the VM is in, etc. To view the variables, hover over the **Info** icon next to **Script**.

Note: Nerdio provides several pre-populated variables that can be used in the script code. The available variables are:

- \$HostPoolId (Available when the script is associated with a host pool)
- \$HostPoolName (Available when the script is associated with a host pool)
- \$AzureSubscriptionId
- \$AzureSubscriptionName
- \$AzureResourceGroupName
- \$AzureRegionName
- \$AzureVMName (Available when the script is associated with a VM)
- \$ADUsername (if passing AD credentials)
- \$ADPassword (if passing AD credentials)
- \$DesktopUser (Available when the script is associated with a personal host pool)



Tips:

- It is advisable to use the Write-Output command throughout the script to provide information about what the script is doing and how far the script has progressed. The output appears in Nerdio Manager. Output from Write-Error also appears, but the output from Write-Verbose does not.
- Have commands that result in an error exit out of the script entirely. In that case, the Run job results in "Fail" instead of "Complete", which is relayed to Nerdio Manager.

```
$errorActionPreference = "Stop"
```

Note: For information about troubleshooting Azure runbooks refer to "Troubleshoot Scripts" on page 190.

Scripted Actions: Azure runbooks variables integration

Nerdio Manager allows you to integrate variables into the Azure runbooks scripted actions. Nerdio Manager prompts the user for these variables when the scripted action is run interactively via the action menu's **Run now** option.

To integrate variables into Azure runbooks scripted actions:

1. Navigate to **Scripted Actions > Azure runbooks**.
2. Locate the scripted action you want to work with.
3. Select **Edit**.
4. In the **Script** section, locate the part of the script that starts with **<# Variables:**.



```
▼ SCRIPT ⓘ  
<# Variables:  
{  
  "InstallPreviewVersions": {  
    "Description": "Set to True to install preview versions of Nerdio Manager",  
    "IsRequired": true,  
    "DefaultValue": "False"  
  }  
}  
#>
```

5. For each variable, enter the following information (see the example below for formatting):

- **Name:** Enter the variable name.

Note: The variable can be something you create, or it can be a Global Secure Variable. See "Scripted Actions Global Secure Variables" on page 189 for details.

- **Description:** Enter the variable's description.
- **IsRequired:** Enter *true* (is required) or *false* (is not required).
- **DefaultValue:** Optionally, enter the variable's default value.

```
<# Variables:
{
  "InstallPreviewVersions": {
    "Description": "Set to True to install preview versions of
Nerdio Manager",
    "IsRequired": true,
    "DefaultValue": "False"
  }
}
#>
```

6. Add, change, or delete the variables as desired.
7. When you have entered all the desired information, select **Save and close**.

Note: When the scripted action is run interactively, a page is displayed that contains the **Parameters** section. All the variables are shown along with their default values and descriptions.

RUN AZURE RUNBOOK SCRIPTED ACTION

Are you sure you want to run this Scripted action Update Nerdio Manager (2)?

Azure subscription

PARAMETERS ⓘ

NAME

VALUE

InstallPreviewVersions

False



Set to True to install preview versions of Nerdio Manager

Add

Variables specified in clear text will be visible in Azure Automation logs. To pass sensitive data use Secure Variables on SETTINGS>Nerdio environment page.

[Show advanced settings](#) ▾

Cancel

Run now

Scripted Actions Global Secure Variables

Nerdio Manager allows you to manage Global Secure Variables. These secure variables can be passed to scripted actions or shell apps. The variables are stored securely in the Azure Key Vault and can be passed to scripted actions using the `$$SecureVars.Variable_Name` variable name.

Tip: This feature is especially helpful if you want to pass sensitive information to a scripted action without passing it via clear text.

To manage global secure variables:

1. Navigate to **Settings > Nerdio environment**.
2. In the **Secure variables** tile, select the action (**add**, **edit**, or **remove**) you wish to perform.
3. To add or edit a global secure variable, enter the following information:

- **Name:** Type the name of the variable.

Note: The variable name must be between 1 and 20 alphanumeric characters.

- **Value:** Type the variable's value.
- **Allow usage within shell apps:** Select this option to make the variable available in Shell Apps.
- **Pass variable to specified scripted actions only:** Optionally, select this option to only pass this variable to the scripted action(s) specified below. When unselected, it is passed to all scripted actions.
 - **Scripted actions:** From the drop-down list, select which scripted action(s) the variable is passed to.

Note: The variable is listed in the **Secure Variables** column of each selected scripted action in the **Azure runbooks** window.

4. When you have entered the desired information, select **OK**.

Troubleshoot Scripts

Azure Runbooks Logs

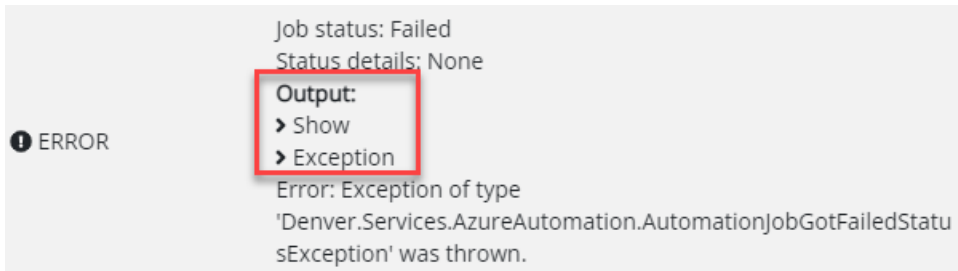
Azure runbooks have enhanced logs that help you troubleshoot issues with scripted actions.

To view the Azure runbook logs:

1. Navigate to **Scripted Actions > Azure runbooks**.
2. At the bottom of the window, in the **Scripted Actions Tasks** section, locate the task with an **Error** in the **Status** column.
3. Select **Details**.

The **Job Details** window displays.

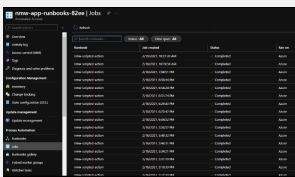
4. Locate the entry in the log with an error.
5. In the **Output** section, select any of the following:

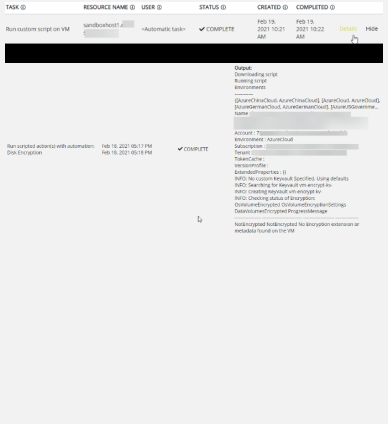
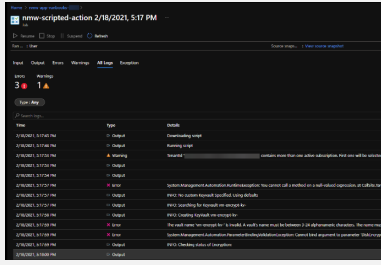


- **Show:** Select **Show** to display the standard Azure automation account runbook output.
- **Exception:** Select **Exception** to display the exception's details.

Troubleshoot Azure Runbooks

Troubleshooting Azure Runbooks

Problem	Solution	Description
In some cases, a script fails to perform the scripted action, but its status is incorrectly set to Complete . This means that the PowerShell script failed to encounter fatal errors. The final output from the script presents information about	<ol style="list-style-type: none"> 1. Navigate to the associated Automation account.  <ol style="list-style-type: none"> 2. View the log with the 	When running an Azure scripted action, the associated Automation account runs a specialized runbook, which copies the code directly from the Nerdio Manager and executes it. All scripts are executed as instances of the same

Problem	Solution	Description
<p>the script but has no indication of an error.</p> 	<p>time stamp that matches the Nerdio Manager task log.</p> <p>3. Find and resolve the error that is produced by the script in your Nerdio Manager.</p>	<p>Automation Account job. Here you can find the errors generated when running your script. The errors vary based on your script.</p> 

Troubleshoot Windows Scripts

For information about troubleshooting Windows scripts refer to [Custom Script Windows - Troubleshoot and Support](#).

For more information about troubleshooting the custom script extension (CSE or CSExtension) refer to [Custom Script Windows - Troubleshoot and Support for Extensions](#).

Tip: It is recommended that you use an isolated development session host and run the scripts directly on the host to test your scripts. This ensures that the PowerShell code is functional and preforms as desired. In addition, it provides quicker results than running the commands through Nerdio Manager.

Troubleshooting Windows Scripts

Problem	Solution	Description
Scripts that cause reboots fail the entire process. When the extension is waiting for the PowerShell script to complete	<p>For actions which require restarts and then additional actions:</p> <ol style="list-style-type: none"> 1. Split the script up into 	N/A

Problem	Solution	Description
fully (and if a reboot is started), the script fails.	<p>multiple scripts.</p> <p>2. Select the "Individual with restart" script execution mode.</p> <p>3. Place the rest of the scripts in order.</p>	

Upgrade Azure Az PowerShell Module

Sometimes a scripted action or PowerShell script that works locally fails in Nerdio Manager with an error such as:

```
Method 'get_SerializationSettings' in type
'Microsoft.Azure.Management.Internal.Resources.ResourceManagementClient'
from assembly 'Microsoft.Azure.PowerShell.Clients.ResourceManager,
Version=1.0.0.0, Culture=neutral, PublicKeyToken=31b57jpo856ad4e35' does not have an
implementation.
```

Sometimes the error message is different, or the error message suggests upgrading your Az modules. These errors can often be resolved by upgrading the Az module or modules used by the scripted action automation account.

To upgrade your Azure Az PowerShell module:

1. Find the scripted actions automation account by selecting the **Browse gallery** button.

Note: Do not use the **Update Az Modules** button because it does not actually update to the latest versions.

2. Search for the relevant Az module, such as **Az.KeyVault**, and upgrade it.

Note: This is determined by the specific command that is failing. For example, if the script fails on **Get-AzKeyVault**, then it is the **Az.KeyVault** module that needs to be updated.

3. Sometimes the modules have dependencies on other Az modules, such as **Az.Accounts**. Dependencies may need to be updated as well.

Note: If you use a hybrid worker to execute scripted actions, then the modules need to be updated on the hybrid worker VM, rather than in the automation account. This can be accomplished using the **Update-Module** command on the hybrid worker VM.

Scripted Actions for Windows Scripts

Windows Scripts are scripted actions that are run directly on the Virtual Machine. They can be thought of as "sign in scripts," except executed machine-wide and performed as part of the provisioning process for creating or removing session hosts, or running commands against the Desktop Image VMs for installing or updating software, or other tasks.

You can create a new scripted action, view, edit, and apply the existing scripted actions. For more information refer to "Scripted Actions Overview" on page 173.

For more information about Scripted Actions for windows refer to [Custom Script for Windows](#).

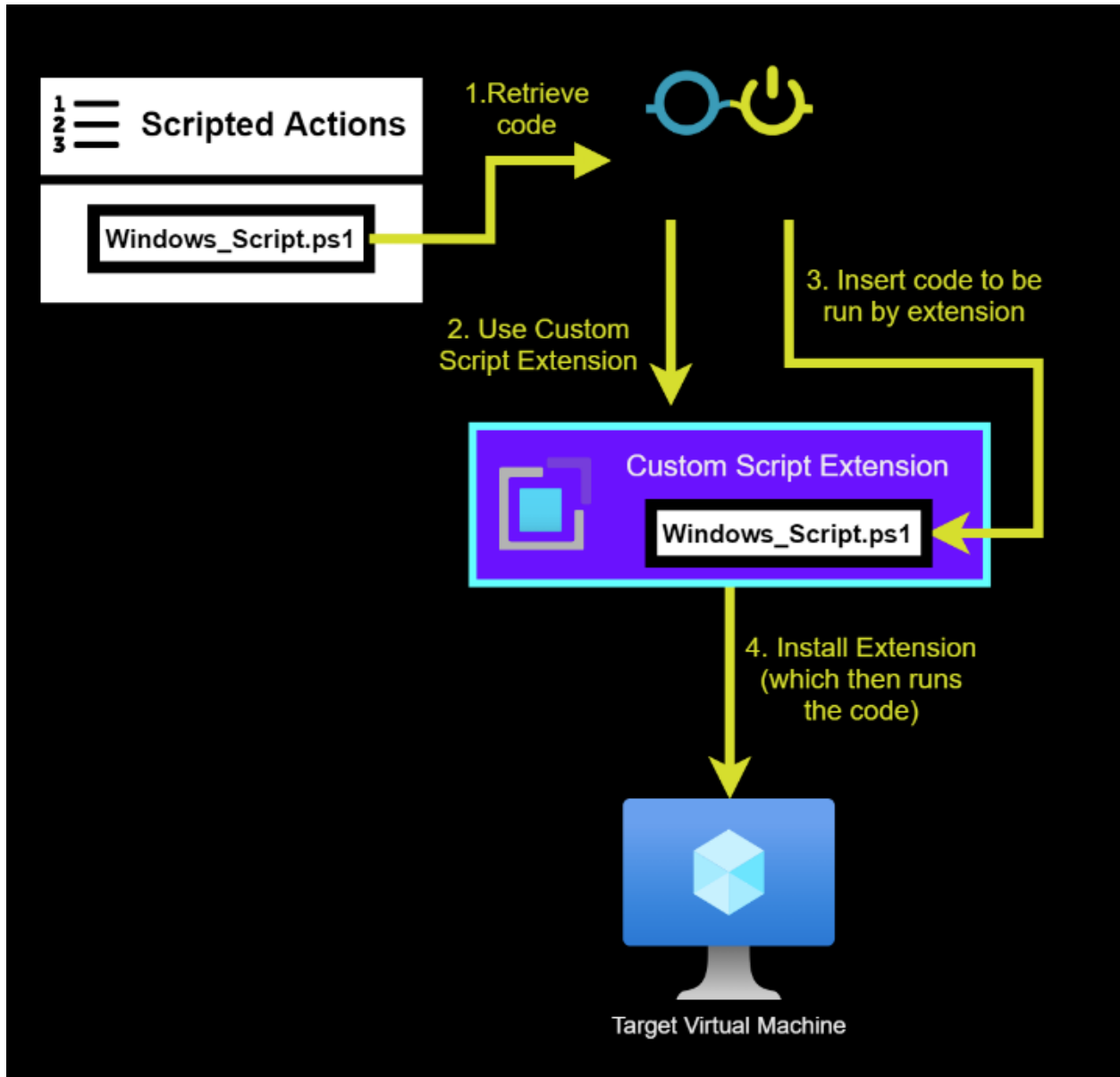
Custom Script Extensions

Nerdio Manager uses the custom script extension to execute PowerShell code on the Virtual Machine.

Notes:

- Nerdio Manager also uses the custom script extension for other tasks. For example, installing FSLogix and AVD agents.
- The script runs with administrative privileges and does not interrupt other sessions. This means that most scripts are safe to run while users are on the VM.

The PowerShell code is taken from the Nerdio Manager scripted actions library, and then passed to the extension to be run on the VM. Certain variables are passed with it (for example, \$DesktopUser). These variables are defined according to the Virtual Machines to which Nerdio Manager is passing the script.



For information about the Windows Scripts CSE troubleshooting refer to [Troubleshoot and Support](#).

For information about troubleshooting for Custom Script Extensions in Nerdio Manager refer to "Troubleshoot Scripts" on page 190.

Related Topics

"Scripted Actions Overview" on page 173

[Custom Script for Windows](#)

[Troubleshoot and Support](#)

"Troubleshoot Scripts" on page 190

"Considerations for Scripted Actions" on page 184

Scripted Actions for Azure Runbooks

Azure Runbooks are Azure Automation Account runbooks that run outside the context of a specific VM. They run directly in your Azure environment through an Azure Automation Account that is created and managed by the Nerdio Manager App in the security context of the Nerdio Manager service principal.

You can create a new scripted action, view, edit, and apply the existing scripted actions. For more information refer to "Scripted Actions Overview" on page 173.

Note: For more information about Scripted Actions refer to "Scripted Actions for Windows Scripts" on page 194.

Azure runbook scripted actions are run via an Automation Account in Azure. This enables automated actions of Azure resources outside of the Virtual Machine.

Notes:

- Azure Runbooks must be enabled manually. For more information about Automation Account refer to [Azure Automation - Overview](#).
- Some of the Azure Runbooks scripted actions are customized by the Nerdio Manager Admin. You can modify the existing script or add your own.
- Each Automation Account is created specifically per an Azure Runbook.

Nerdio Manager allows you to leverage dedicated hybrid worker VMs to integrate Azure Automation accounts with environments that require private endpoints. Hybrid worker VMs are connected directly to a VNet and scripted actions can be used when Key Vault and other Nerdio Manager components are only accessible via private endpoints.

Before you can implement hybrid workers in Nerdio Manager, you must do the following:

- Create an extension-based hybrid worker .See this Microsoft [document](#) for details.
- Install the Run As account certificate on the hybrid worker. See "Install the Run As account certificate on the hybrid worker:" below below for details.

To configure the Azure runbooks settings:

1. Navigate to **Settings > Nerdio environment**.
2. In the **Azure runbooks scripted actions** tile, select **Enabled** or **Disabled** (depending on the current status).
3. Enter the following information:
 - **Use Azure Automation Runbooks?:** Toggle this option on or off.
 - **Off:** The Automation Account is deleted when you disable this feature.
 - **On:** You can select an Azure region where an Automation Account is created to run this Runbook.
 - **Automation Account Name:** Type the account name. This is a unique name and is only used to run these Azure Runbooks.
 - **Hybrid Worker Group:** Optionally, from the drop-down list, select the hybrid worker group.
4. Once you have entered the desired information, select **OK**.

Install the Run As account certificate on the hybrid worker:

Note: See this Microsoft [document](#) for details.

1. Find the Azure Key vault associated with the Nerdio installation. It begins with **nmw-app-kv-**.
2. In the **Key Vault**, select **Certificates**.
3. Select the certificate called **nmw-scripted-action-cert**.

4. Select Download in **PFX/PEM format**.

Note: In order to download the certificate, your user account needs permission to list/get certificates AND secrets from the key vault. See this Microsoft [article](#) for more information.

5. Install the downloaded certificate on the hybrid worker VM.

Renew the Azure Runbook Scripted Actions Automation Certificate

Nerdio Manager allows you to renew the Azure Runbook scripted actions automation certificate.

To renew the certificate:

1. Navigate to **Settings > Nerdio environment**.
2. In the **Azure runbooks scripted actions** tile, select **Renew certificate**.
3. **Certificate Validity (Months)**; Type the desired number of months.

Note: The default value of 120 months is recommended.

4. Once you have entered the desired information, select **OK**.

Note: This task may take some time to run. You can follow its progress in the **Settings Tasks** window.

5. After you renew the certificate, be sure to connect the subscriptions.
 - In the **Azure runbooks scripted actions** tile, select **connect** for each subscription that is not connected.
 - Follow the on-screen instructions to connect each subscription.

Related Topics

"Scripted Actions Overview" on page 173

"Scripted Actions for Windows Scripts" on page 194

"Considerations for Scripted Actions" on page 184

Scripted Actions for Windows 365

This is an overview about how to use scripted actions in the context of Windows 365.

Important! Before you start this topic, be sure that you have read [Windows 365 Enable and Configure Cloud PCs](#).

Note: Nerdio Manager is set up so that you can use the same scripts for AVD and Windows 365 without any significant modifications.

To add a new scripted action:

1. Navigate to **Scripted Actions > Windows scripts**.

Note: Only Windows scripts are relevant for Windows 365 scripted actions.

2. Select **Add scripted action**.
3. Enter the following information:
 - **Name:** Type the script's name.
 - **Description:** Type the script's description.
 - **Tags:** From the drop-down list, select the tag(s). Alternatively, type a new tag.
 - **Script Executing Mode:** From the drop-down list, select the script's execution mode.
 - **Enable Cloud PC:** You must select this option to enable this script for Windows 365.
 - **Run this script using the logged on credentials:** Select this option to run the script with the user's credentials. Otherwise, the script runs in the system context.

- **Enforce script signature check:** Select this option to force the script to be signed by a trusted publisher. Otherwise, no warning or prompt displays and the script runs unblocked.
- **Run this script in 64 bit PowerShell host:** Select this option to run the script in 64-bit PowerShell host for a 64-bit client architecture. Otherwise, the script runs in 32-bit PowerShell host.
- **Assign to all users:** Optionally, assign the scripted action to all users.
- **Assign to all devices:** Optionally, assign the scripted action to all devices.
- **Assign to selected groups:** Optionally, assign the scripted action to selected groups. (Recommended)
- **Exclude assignments:** Optionally, exclude members in the selected groups from applying the scripted action.

Note: Cloud PC security works with user groups and not with individual users.

- **Script:** Type or copy/paste the script.
4. Once you have entered all the desired information, select **OK**.


Notes:

- The script is now enabled for Cloud PC and is submitted to run on the Cloud PCs. **This could take quite a long time to finish, possibly several hours.**
- In the Windows Scripts list, the **Applied To** column is updated with the number of devices this script applies to.

APPLIED TO ⓘ

Host pools: 1
Desktop images: 0 Edit ▾

Host pools: 1
Desktop images: 0
Cloud PCs: 10 Edit ▾



- Select the number to see the detail log information.

DEVICE NAME	USER	LAST UPDATE	RESULT
CPC-adalvi-8-LR		Success Sep 22, 2021 07:59 AM	
CPC-bvankaam-EQ		Success Sep 22, 2021 07:32 AM	
CPC-sbhujbal-4C		Success Sep 22, 2021 07:32 AM	
CPC-adalvi-H-UG		Success Sep 22, 2021 06:58 AM	
CPC-vladimi-U5		Success Sep 22, 2021 06:47 AM	
CPC-clong-2S-R0		Success Sep 22, 2021 06:41 AM	
CPC-nmclough-9V		Success Sep 22, 2021 06:20 AM	

- In addition, you can navigate to **Windows 365 > Cloud PCs**. The **Scripts** column shows you all the scripts that have executed on the Cloud PC. Select any script to see its detail log information.

SCRIPTS

Install Microsoft 365 Office
Apps
Install Zoom VDI client
Install Remote Display
Analyzer
more...

Host Pools

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

After you create the desktop images, the next step in the Nerdio Manager AVD deployment flow is to create host pools from the desktop images.

Host pools are groups of identical Azure VMs that host the Azure Virtual Desktops that end users sign in to. All VMs in the host pool share a set of configuration options: VM size, OS disk size, base image, AD domain, user profile storage location, and more.

You can configure two types of host pools:

- **Static:** A static host pool contains a set number of session hosts that the administrator configures. That is, it does not have auto-scale enabled.

Note: When Nerdio Manager is first deployed to an **existing** environment, the host pools that are created are static host pools. They can be converted to dynamic host pools.

- **Dynamic:** A dynamic host pool is a host pool whose configuration can be scaled in and out (auto-scale) as per the workload. That is, auto-scale can create the session hosts automatically based on the auto-scale configuration.

Related Topics

"Create Static Host Pools Without Auto-Scaling" on page 206

"Create Dynamic Host Pools" on page 214

Delete Hosts, Host Pools, and Workspaces

"Convert a Static Host Pool to Dynamic" on page 211

Workspace Management

A workspace is a container for host pools and session hosts that provide desktops and RemoteApps to users. This topic discusses creating and managing workspaces.

Create a Workspace

A workspace must be created before you can create host pools and session hosts.

To create a workspace:

1. Navigate to **Workspaces**.
2. Select **Add Workspace**.
3. Enter the following information:

- **Name:** Type the workspace's name.

Note: The Name is assigned to the workspace during creation and cannot be changed later. By default, it is visible to the end-user. Specifying a Friendly Name overrides what is visible to the end-user.

- **Friendly Name:** Type the Friendly Name.
- **Description:** Type the description, which is only visible to admins.
- **Resource group:** From the drop-down list, select the resource group to contain the workspace.
- **Location:** From the drop-down list, select the Azure location for the workspace's objects and associated metadata.
- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the Workspace.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

4. Once you have entered all the desired information, select **OK**.

The workspace is created.

Manage Workspaces

From the Workspaces table, you can do the following:

- **Dynamic host pools:** Manage the workspace's dynamic host pools.
- **Static host pools:** Manage the workspace's static host pools.
- **Unassign:** Unassign the workspace from Nerdio Manager.
- **Delete:** Delete a Workspace.

Note: You may only delete a workspace that has no host pools.

- **User Sessions:** Manage the workspace's user sessions.

Create Static Host Pools Without Auto-Scaling

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

The following procedure allows you to create a new static host pool.

To create a new static host pool:

1. Navigate to **Workspaces**.
2. Select the workspace you wish to work with.
3. Navigate to **Workspaces > Static Host Pools**.
4. Select **Add static host pool**.

5. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 86 for details.

- **Name:** Type the name of the static host pool.
- **Description:** Type the host pool's description.

Note: Optionally, select **Generate using AI** to have AI create the description. See Overview of AI-Powered Description Generation for details.

- **Resource Group:** From the drop-down list, select the resource group for the host pool.
- **Desktop Experience:** From the drop-down list, select the desktop experience.

Note:

- **Multi user desktop (pooled):** This is the full desktop experience. Users are not assigned to individual session hosts and are placed on a host based on its load. Multiple users are pooled together on a group of hosts.
- **Multi user RemoteApp (pooled):** This is only published applications, not a full desktop experience. Published RemoteApps are visible to users as native apps running on their local computer. The RemoteApps are provided by a collection (pool) of session hosts.
- **Single user desktop (pooled):** This is the full desktop experience. Users are placed on individual desktop VMs (one user per session host) and a preconfigured number of spare(available) desktops is maintained.
- **Single user desktop (personal):** This is a personal (persistent) full desktop experience. A dedicated session host VM is assigned to each user.

- **Directory:** From the drop-down list, select the directory.

Note: The default option is the global default Nerdio Manager AD configuration. To use a custom configuration for the host pool, select the **Custom** option.

- **FSLogix:** From the drop-down list, select the FSLogix configuration profile to be used when creating or re-imaging hosts in this host pool.
- **RDP Profile:** From the drop-down list, select the RDP profile.
- **Initial Host Count:** Type the number of sessions hosts to add to the host pool during creation.

Note: Static host pools can be created with zero or more session hosts. New session hosts can be added or deleted at any time.

- **Name:** Type the name of the newly added hosts for the Exact name, a Prefix or the Prefix+Pattern.
 - **Exact/Prefix/Pattern:** From the drop-down list, select whether to use an Exact name, a Prefix, or a Pattern.

Note:

- **Exact** applies when adding a single host and specifying an exact name. For example, MYADVHOST.
- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
- **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network. The network determines the Azure region of the VM.

Note: The network is the Azure VNETS and subnets. If it is not present in the list, it must be added in **Settings > Azure environment > Linked networks**.

- **Desktop Image:** From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.

- **VM Size:** From the drop-down, select the VM disk size and type for newly created session hosts.

Note: If any VM size is not available for a subscription or region, it doesn't appear in the list. At times, even if a VM size is available in a specific Azure region, it cannot be used due to the subscription having restrictions on a particular size. In such cases, we show the VM size in the drop-down list, but don't allow users to select it (the size is disabled).

- **OS Disk:** From the drop-down list, select the OS Disk type and size for newly created session hosts.

Note: This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S-type) is not recommended. Premium SSD provides best performance.

- **Resource Group:** From the drop-down list, select the resource group to contain the VMs.
- **Quick Assign:** From the drop-down list, select the users or groups to pre-assign to newly created desktops.

Note: The number of users specified cannot exceed the number of hosts being added. User assignment can be modified after the host pool is created.

- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the host pool.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

- **Add "cm-resource-parent" tag:** Select this option to add the "cm-resource-parent" tag to the host pool.
 - **App group settings:** Optionally, type the **App group name** of the host pool.
 - **Application policies:** Optionally, select the application policies to assign to the host pool.
6. Once you have entered all the desired information, select **OK**.

The process of host pool creation begins. First a host pool itself is created, then session host VMs are built out. Session hosts are joined to Active Directory, AVD and FSLogix agents are installed on the session hosts and users/groups are assigned per the configuration you selected.

Note: You can convert a static pool into a dynamic pool. For more information refer to "Convert a Static Host Pool to Dynamic" below.

Related Topics

"Host Pools" on page 204

"Create Dynamic Host Pools" on page 214

Delete Hosts, Host Pools, and Workspaces

"Convert a Static Host Pool to Dynamic" below

Convert a Static Host Pool to Dynamic

The following procedure allows to a user to convert a static host pool to a dynamic host pool. The dynamic host pool can then be configured for auto-scaling.

To convert a static host pool to dynamic:

1. Locate the static host pool you wish to convert.
2. Select **Convert to Dynamic**.
3. On the confirmation window, select **Confirm**.

Note: By default, the auto-scale option for this host pool is off. This new host pool has no user sessions. You can manually add and remove hosts to and from the pool. Alternatively, you can enable auto-scale. See "Enable Dynamic Host Pool Auto-scaling" on page 219 for details.

Add a New Session Host to a Static Host Pool

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

Once a host pool is created, you can manually add session hosts.

To add a session host to a static host pool:

1. Locate the static host pool you wish to work with.
2. From action menu, select **Hosts > Add new**.
3. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 86 for details.

- **Host Count:** Type the number of session hosts to add to the host pool.
- **Host Name:** Type the name of the newly added hosts for the Exact name, a Prefix or the Prefix+Pattern.
 - **Exact/Prefix/Pattern:** From the drop-down list, select whether to use an Exact name, a Prefix, or a Pattern.

Note:

- **Exact** applies when adding a single host and specifying an exact name. For example, MYADVHOST.
 - **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
 - **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{####} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{????} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network. The network determines the Azure region of the VM.
 - **Desktop Image:** From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.

Note: The **Unmanaged Azure Compute Gallery image versions** section is at the bottom of the list. These are unmanaged, backup versions of images that were created while activating staged images. These images can be used to restore any changes made to session hosts.

- **VM Size:** From the drop-down, select the VM disk size and type for newly created session hosts.

- **OS Disk:** From the drop-down list, select the OS Disk type and size for newly created session hosts.

Note: This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S-type) is not recommended. Premium SSD provides best performance.

- **Resource Group:** From the drop-down list, select the resource group to contain the VMs.
- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the session host.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

- **Schedule:** Optionally, toggle on the schedule, and enter the schedule information, to run this job per the schedule.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Create Dynamic Host Pools

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

The following procedure allows you to create a new dynamic host pool.

To create a new dynamic host pool:

1. Navigate to **Workspaces**.
2. Select the workspace you wish to work with.
3. Navigate to **Workspaces > Dynamic Host Pools**.
4. Select **Add dynamic host pool**.
5. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 86 for details.

- **Name:** Type the name of the host pool.
- **Description:** Type the host pool's description.

Note: Optionally, select **Generate using AI** to have AI create the description. See Overview of AI-Powered Description Generation for details.

- **Resource Group:** From the drop-down list, select the resource group for the host pool.
- **Desktop Experience:** From the drop-down list, select the desktop experience.

Note:

- **Multi user desktop (pooled):** This is the full desktop experience. Users are not assigned to individual session hosts and are placed on a host based on its load. Multiple users are pooled together on a group of hosts.
- **Multi user RemoteApp (pooled):** This is only published applications, not a full desktop experience. Published RemoteApps are visible to users as native apps running on their local computer. The RemoteApps are provided by a collection (pool) of session hosts.
- **Single user desktop (pooled):** This is the full desktop experience. Users are placed on individual desktop VMs (one user per session host) and a preconfigured number of spare(available) desktops is maintained.
- **Single user desktop (personal):** This is a personal (persistent) full desktop experience. A dedicated session host VM is assigned to each user.

- **Directory:** From the drop-down list, select the directory.

Note: The default option is the global default Nerdio Manager AD configuration. To use a custom configuration for the host pool, select the **Custom** option.

- **FSLogix:** From the drop-down list, select the FSLogix configuration profile to be used when creating or re-imaging hosts in this host pool.
- **RDP Profile:** From the drop-down list, select the RDP profile.
- **Name:** Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
 - **Prefix/Pattern:** From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
 - **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network. The network determines the Azure region of the VM.

Note: Nerdio Manager verifies that there is a sufficient number of available IP addresses on the selected network before deploying new host pool VMs. If there are insufficient available IP addresses, an error message is displayed and you may not add the new host pool.

- **Desktop Image:** From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.
- **VM Size:** From the drop-down, select the VM disk size and type for newly created session hosts.

Note: If any VM size is not available for a subscription or region, it doesn't appear in the list. At times, even if a VM size is available in a specific Azure region, it cannot be used due to the subscription having restrictions on a particular size. In such cases, we show the VM size in the drop-down list, but don't allow users to select it (the size is disabled).

- **OS Disk:** From the drop-down list, select the OS Disk type and size for newly created session hosts.

Note: This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S-type) is not recommended. Premium SSD provides best performance.

- **Resource Group:** From the drop-down list, select the resource group to contain the VMs.
- **Quick Assign:** From the drop-down list, select the users or groups to pre-assign to newly created desktops.

Note: The number of users specified cannot exceed the number of hosts being added. User assignment can be modified after the host pool is created.

- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the host pool.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

- **Add "cm-resource-parent" tag:** Select this option to add the "cm-resource-parent" tag to the host pool.
- **App group settings:** Optionally, type the **App group name** of the host pool.

- **Application policies:** Optionally, select the application policies to assign to the host pool.
 - **Validation environment:** Select this option to receive service updates at a faster cadence than non-validation host pools, allowing you to test service changes before they are deployed broadly to production.
6. Once you have entered all the desired information, select **OK**.
 7. The auto-scale configuration window displays. If desired, configure the auto-scaling for the host pool. See "Enable Dynamic Host Pool Auto-scaling" below for more information.

The process of host pool creation begins. If auto-scaling has been enabled, it may take some time to complete. Otherwise, the host pool is created immediately. This creates an "empty" host pool - there are no session hosts in that host pool. An end-user who attempts to connect to the empty host pool is informed that there are no resources (that is, session hosts) to serve up a desktop. You can monitor progress in the **Host Pools Tasks** section.

Related Topics

"Enable Dynamic Host Pool Auto-scaling" below

"Host Pools" on page 204

"Create Static Host Pools Without Auto-Scaling" on page 206

Delete Hosts, Host Pools, and Workspaces

Enable Dynamic Host Pool Auto-scaling

The auto-scale feature ensures that only the number of session host VMs required to serve the current demand are running. When not in use, VMs are stopped or deleted. When demand rises, or at specific times of the day, additional VMs in the host pool are started or created. This allows for cost savings.

You can enable and configure the auto-scaling feature for dynamic host pools.

Note: By default, the **Auto-scale** option is disabled. When you enable auto-scaling, you can configure the desktop image, VM size, and OS disk template, and also set the criteria for host pool sizing, scaling logic, and pre-stage hosts.

To enable dynamic host pool auto-scaling:

1. Locate the dynamic host pool you wish to work with.
2. From the action menu, select **Auto-scale > Configure**.
3. Enter the following basic auto-scale information:
 - **Auto-Scale:** Toggle this option **On**.
 - **Auto-scale Timezone:** From the drop-down list, select the time zone for the auto-scale process.
 - **Name:** Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
 - **Prefix/Pattern:** From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
 - **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network the VM connects to.

Note: The VM that is created on the selected network is created in the Azure region associated with the network.

- **Desktop Image:** From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **VM Size:** From the drop-down list, select the VM size for new session hosts.
- **Running OS Disk (Template):** From the drop-down list, select the OS disk type and size for new session hosts.
- **Stopped OS Disk Type:** From the drop-down list, select the OS disk type when session host VMs are stopped.

Note: See [Auto-Scale Cost Optimization OS Disk Storage](#) for more information about OS disk auto-scale configuration.

- **Resource Group:** From the drop-down list, select the resource group where VMs should be created.
- **VM Naming:** From the drop-down list, select the VM naming to use.

Note: Host VMs that are created automatically by the scale out or auto-grow process use names based on the selected VM naming mode. See [How Session Host VM Names are Generated](#) for more information.

- **Re-use names:** Always attempt to re-use names that were previously used in the pool, if available.
 - **Standard names:** Use the next available name.
 - **Unique names:** Always attempt to use a unique name for new hosts.
- **Automatically Re-image Used Hosts:** Selecting this option to re-image hosts that had at least one user logged into them. For multi-session hosts, the hosts are re-imaged once the last user signs out.

4. Select the **Default schedule** or **Alternative schedule**.

Note: Nerdio Manager allows you to configure separate auto-scale settings for a default schedule (normal operations) and an alternative schedule (outside of normal operations). For example, you may want fewer session hosts available on weekends or bank holidays. Alternatively, you may want more session hosts available two weeks prior to Christmas when you have a large number of temporary customer support agents. In either case, you would use the **Alternative schedule** tab to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, navigate to the **Alternative schedule** tab and enter the following information:

Note: The Estimated Monthly Costs shown at the top of this page only consider the Default Schedule's settings.

- **Schedule:** Toggle on the Schedule option to turn on the Alternative Schedule process.
 - **Days:** From the drop-down list, select the off-peak day(s).
 - **Dates:** Select the specific off-peak date(s).
 - Select **+** or **-** to add or remove off-peak dates.
5. Select the **Auto-scale profile (Premium only)**:
- From the drop-down list, select the auto-scale profile to use. Alternatively, select **Custom** to create a custom auto-scale configuration.

Note: See Manage Auto-scale Profiles for details about creating and working with auto-scale profiles.

6. Enter the following **Host Pool Properties** information:
- **Session limit host:** Type the maximum number of sessions per host. Once this session limit is reached, and there are no more available hosts, a new host is started automatically, if it exists.
 - **Load Balancing:** From the drop-down list, select the desired load balancing.

Note:

- **Breadth First** means that the load-balancing algorithm spreads the users evenly across all available session hosts.
- **Depth First** means the load-balancing algorithm places all the users in the first session host until the host's session limit is reached. Only then, does it place the users in the next session host. If necessary, it powers on the VM and makes it available to the users.

- **Start on connect:** Select this option to start the session host VMs on connect.

7. Enter the following **Host Pool Sizing** information:

- **Active Host Defined As:** From the drop-down list, select the active host definition.

Note: When set to "VM started," the system identifies a session host VM as active as long as the VM is running in Azure. There are very few instances when "VM started" should be selected.

When set to "AVD Agent Available," the system identifies a session host VM as active only when the AVD back-end is receiving heartbeats and sees the session host as "Available." In general, you should select "AVD Agent Available."

- **Base Host Pool Capacity:** Type the number of session host VMs to always be part of this host pool. These session hosts may be stopped or running.
- **Min Active Host Capacity:** Type the minimum number of running session hosts that are always available. Typically, a session host must be running for users to sign in or the "Start on connect" feature is enabled. Other VMs can be either stopped or turned on, as configured by the user auto-scaling logic.
- **Burst Beyond Base Capacity:** Type the capacity to burst above the standard number of session host VMs when there is user demand. The system automatically creates up to this number of new session host VMs above the **Base Host Pool**

Capacity, when needed. These session hosts are the first ones to be removed when the system scales in after business hours.

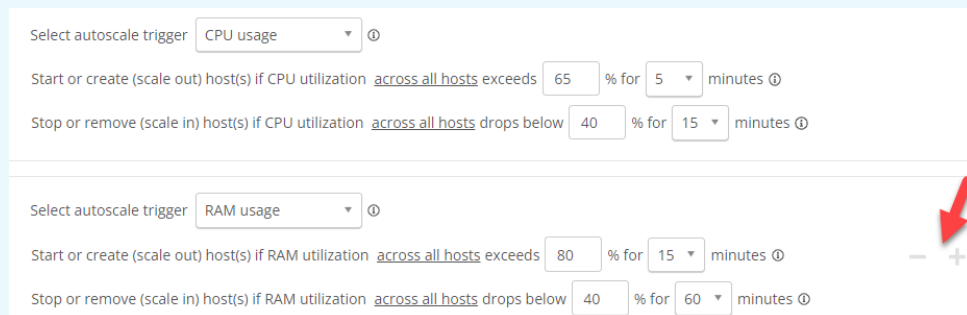
8. Enter the following **Scaling Logic** information:

- **Use Multiple Auto-scale Triggers:** Select this option to enable multiple usage triggers to be used for scaling out and scaling in.

The multiple auto-scale triggers feature is only available in the Nerdio Manager Premium edition.

Notes:

- Auto-scale adds capacity when **any** of the scale out conditions are met. Capacity is removed only when **all** the scale in conditions are met.
- Use the + and - buttons to add or remove scale out triggers. You may select up to 3 triggers.



Select autoscale trigger CPU usage % for minutes % for minutes

Select autoscale trigger RAM usage % for minutes % for minutes

- **Select Auto-scale Trigger:** From the drop-down list, select the auto-scale trigger.

Note: The available triggers are:

- **CPU usage or RAM usage:** This scales out when the average CPU or RAM usage across all running session hosts in the pool exceeds a predefined value for a predefined duration.
- **Average active sessions:** This scales out when the average number of active sessions per host exceeds a predefined value.
- **Available sessions:** This maintains the number of available hosts by scaling out and scaling in within the limits of the Host Pool Sizing and the maximum number of sessions per host.
- **User-driven:** Hosts are started when users connect and are automatically stopped after a defined amount of time after all users sign out.

- For **CPU usage or RAM usage:**
 - **Start or Create (Scale Out) Up To:** Scale out by starting (if there are stopped VMs) or creating (if there are no stopped VMs) session hosts if the trigger is exceeded.
 - **Stop or Remove (Scale In) Up To:** Scale in by stopping (if there are no burst VMs) or removing (if there are burst VMs) session hosts if scale in trigger is met.
- For **Average active sessions:**
 - **Start or Create (Scale Out) Up To:** Scale out by starting (if there are stopped VMs) or creating (if there are no stopped VMs) session hosts if the average active sessions across all hosts is exceeded.
 - **Stop or Remove (Scale In) Up To:** Scale in by stopping (if there are no burst VMs) or removing (if there are burst VMs) session hosts if if the average active sessions across all hosts is below the number specified.
- For **Available sessions:**

- **Maximum sessions per host:** Type the maximum sessions per host.
- **Maintain up to X available sessions:** Type the number of sessions that must be available either always or during work hours.

Note: This ensures that there are this many available sessions during work hours or at all times. Work hours start at **Start of work hours** specified in the **Pre-Stage Hosts** section and end at the beginning of scale in period specified in the Scale in restrictions section below.

- **Outside work hours:** Type the number of sessions to maintain outside of work hours.

Note: This value cannot exceed the number of desktops available during work hours.

- **Working hours:** From the drop-down lists, select the start and end times for working hours.
- **For User Driven:**
 - **When all users log off, scale in hosts after:** From the drop-down list, select the number of minutes to scale in after all users have signed out.

Note: Desktops are automatically stopped only when there are no active or disconnected sessions. To automatically sign out disconnected users after a certain time, use the user session limits settings on the host pool properties.

- **Scale in Restrictions:**
 - **Stop or Remove (Scale In) Hosts Only From:** From the drop-down list, select the time to perform the scale in operation. Select **<any time>** to allow scaling in to be performed at any time.

- **Scale In Aggressiveness:** From the drop-down list, select the scale in aggressiveness.

Note:

- **High Aggressiveness:** Scale in aggressiveness is set to **High** by default, which means it is guaranteed that after business hours, hosts that have active or disconnected sessions running on them are automatically deleted or powered off to reduce capacity. After business hours, the auto-scale logic first removes the hosts that have no sessions running on them. The remaining hosts are sorted based on the least number of sessions running on them. The users with active sessions are then consolidated and moved to a single host and the other hosts are removed by auto-scale. A warning message is sent to the active session users before removing the session hosts.
 - **Medium Aggressiveness:** When scale in aggressiveness is set to **Medium**, after business hours, the scaling logic only removes the hosts that have disconnected sessions running on them. The session hosts with active sessions running on them won't be removed. In this case, the host pool is scaled in to some extent.
 - **Low Aggressiveness:** When scale in aggressiveness is set to **Low**, after business hours, the scaling logic only removes those session hosts that have absolutely no sessions running on them. The auto-scale logic does not remove any session host that have sessions, either active or disconnected, running on them. Though this option is less disruptive for the users, there is no guarantee that the host pool is ever scaled in.
- **Deactivate (drain mode) hosts:** Optionally, you can tell the auto-scale engine to deactivate all hosts at the start of the scale in window. It does leave the minimum number of hosts as specified in the **Min active host capacity** in the **Host Pooling Size** section.

9. Enter the following **Rolling Drain Mode** information:

Notes:

- You can create multiple drain windows and target a specific percentage of your hosts to drain mode, outside of the Scale-in Restriction window. This feature allows you to prevent new connections to a percentage of hosts and allows these hosts to be shut down more quickly, saving on resource costs.
- Rolling drain mode selects hosts to scale in as follows:
 - First, it starts with lowest active sessions.
 - Then it scales in hosts that are already in drain mode,
 - Finally, it scales in hosts with the lowest number of total sessions (active + disconnected).
- **Rolling Drain Mode:** Toggle this option on to enable rolling drain mode.
- **Window name:** Type the name for this drain window.
- **Start time:** From the drop-down lists, select the start time when this drain window comes into effect.

Note: The last drain window remains in effect until 11:59 PM.

- **% hosts in drain mode:** Type the percentage of hosts in drain mode during this window.

Note: Use to add or remove drain windows.

- **Load balancing:** From the drop-down list, select the preferred load balancing algorithm.

Note: This option is only available in the Nerdio Manager **Premium** edition.

- **Depth First:** The load balancing algorithm places users on a single host until the session limit is reached, at which point users start being placed on the next host until the session limit is reached again.
 - **Breadth First:** The load balancing algorithm spreads users evenly across available session hosts.
-
- **Scale in aggressiveness:** From the drop-down list, select the scale in aggressiveness.

Note: See the details in the **Scale in Restrictions** section above.

10. Enter the following **Pre-Stage Hosts** information:

Note: Configure the system to automatically pre-stage some hosts as available capacity with respect to the business hours. For example, you can pre-stage hosts at the beginning of the work day, so the system does not have to auto-scale in real time for users who all sign in at the same time when they start work.

- **Use Multiple Schedules:** Select this option to enable multiple, non-overlapping pre-staging schedules to be used.

Note: This is not available for the Available Sessions trigger when During Work Hours option is specified.

- **Work Days:** From the drop-down list, select the work days when pre-stage tasks should be run.
- **Start of Work Hours:** From the drop-down select the starting hour when pre-stage tasks should be run.

- **Host to be Active by Start of Work Hours:** Type the number of session hosts that should be ready to accept user connections by this time.
- **Scale In Delay:** From the drop-down list, select a delay to restrict scale in operations after the start of work hours. Pre-staged hosts are not scaled in during this time even if they are unused.

11. Enter the following **Messaging** information:

Note: The system sends messages to any users connected to a session host that has been selected for scale in.

- **Send a Warning Message to Users on the host:** From the drop-down list, select the number of minutes before scaling in that the message should be sent.
- **The message should say:** Type the warning message text.

12. Enter the following **Auto-Heal Broken Hosts** information:

Note: Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts:** Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is:** From the drop-down lists, select the desired statuses along with the sessions status.

Note: The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft [article](#) for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

- **Minutes before first action:** Type the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

Notes:

- You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
 - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.
- **Minutes between recovery actions:** Type the number of minutes to wait after each restart attempt before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

Note: If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

13. Once you have entered all the desired information, select **Save** or **Save & close**.

Related Topics

"Create Dynamic Host Pools" on page 214

"Enable Personal Host Pool Auto-scaling" on the next page

Enable Personal Host Pool Auto-scaling

Nerdio Manager allows you to perform auto-scaling on personal host pools. This enables you to do the following:

- Personal desktops can be automatically powered on and off based on a schedule. Alternatively, personal desktops can be stopped when there are no active or disconnected sessions.
- The host OS disk type can be changed to a lower priced storage type when the personal desktop is not running.
- Auto-healing automatically attempts to repair "broken" session hosts. In addition, it allows scripted actions, such as SxS re-install or AVD host re-register, to be executed against them.

To configure the basic auto-scale information:

1. Locate the personal host pool you wish to work with.
2. From the action menu, select **Auto-scale > Configure**.
3. **Auto-Scale**: Toggle this option **On**.
4. Enter the following basic auto-scale information:
 - **Auto-scale Timezone**: From the drop-down list, select the time zone for the auto-scale process.
 - **Name**: Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
 - **Prefix/Pattern**: From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
 - **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network the VM connects to.

Note: The VM that is created on the selected network is created in the Azure region associated with the network.

- **Desktop Image:** From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **VM Size:** From the drop-down list, select the VM size for new session hosts.
- **Running OS Disk (Template):** From the drop-down list, select the OS disk type and size for new session hosts.
- **Stopped OS Disk Type:** From the drop-down list, select the OS disk type when session host VMs are stopped.
- **Resource Group:** From the drop-down list, select the resource group where VMs should be created.

- **VM Naming:** From the drop-down list, select the VM naming to use.

Note: Host VMs that are created automatically by the scale out or auto-grow process use names based on the selected VM naming mode. See How Session Host VM Names are Generated for more information.

- **Re-use names:** Always attempt to re-use names that were previously used in the pool, if available.
- **Standard names:** Use the next available name.
- **Unique names:** Always attempt to use a unique name for new hosts.

5. Select the **Default schedule** or **Alternative schedule**.

Note: Nerdio Manager allows you to configure separate auto-scale settings for a default schedule (normal operations) and an alternative schedule (outside of normal operations). For example, you may want fewer session hosts available on weekends or bank holidays. Alternatively, you may want more session hosts available two weeks prior to Christmas when you have a large number of temporary customer support agents. In either case, you would use the **Alternative schedule** tab to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, navigate to the **Alternative schedule** tab and enter the following information:

Note: The Estimated Monthly Costs shown at the top of this page only consider the Default Schedule's settings.

- **Schedule:** Toggle on the Schedule option to turn on the Alternative Schedule process.
- **Days:** From the drop-down list, select the off-peak day(s).

- **Dates:** Select the specific off-peak date(s).
- Select **+** or **-** to add or remove off-peak dates.

6. **Auto-scale Mode:** From the drop-down list, select the desired auto-scale mode.

Notes:

- **User-driven:** The auto-scaling is performed when there are no active or disconnected sessions.
- **Schedule-based:** The auto-scaling is performed as per the specified schedule.

7. **Auto-scale profile (Premium only):** Optionally, from the drop-down list, select the auto-scale profile to use. Alternatively, select **Custom** to create a custom auto-scale configuration.

Note: See Manage Auto-scale Profiles for details about creating and working with auto-scale profiles.

8. Continue the configuration process with the relevant auto-scale mode:

- **User-driven:** See "To enable user-driven personal host pool auto-scaling:" below
- **Schedule-based:** "To enable schedule-based personal host pool auto-scaling:" on page 244

To enable user-driven personal host pool auto-scaling:

1. **Auto-scale Mode:** From the drop-down list, select the **User-driven**.
2. Enter the following **Host Pool Properties** information:
 - **Start on connect:** Select this option to start the desktop on connect.
3. Enter the following **Desktop Start and Stop** information:

- **Desktop Start and Stop:** Toggle this option on to enable desktop start and stop.
- **Desktops are stopped when users log off after:** From the drop-down list, select the number of minutes or hours to scale in after all users have signed out.

Notes:

- Desktops are automatically started when users connect.
 - Desktops are automatically stopped only when there are no active or disconnected sessions. To automatically sign out disconnected users after a certain time, use the user session limits settings on the host pool properties.
- **Bypass drain mode for desktops in this pool:** Select this option so that desktops do not enter drain mode before shutdown.
4. Enter the following **Pre-stage hosts** information:
- **Pre-stage Host OS Disks:** Toggle this option on to enable pre-staging OS disks.

Note: When pre-stage hosts is enabled it take precedence on other user-driven configuration. Stopped hosts will be started, hosts in drain mode will be activated, stopped disk types will be changed to running, and hosts will not be stopped or deactivated even if there are no user sessions.

- Select the box to include hosts without assigned users.
- **Work days:** From the drop-down list, select the workdays when large numbers of users log into their virtual desktops or applications at the same time.
- **Start of work hours:** Select the time in the morning when users start logging into their virtual desktops or applications.
- **Scale in delay:** Select a delay to restrict scale in operations after the start of work hours.

Note: Pre-staged hosts will not be scaled in during this time even if they are unused.

5. Enter the following **Pre-stage Host OS Disks** information:

- **Pre-stage Host OS Disks:** Toggle this option on to enable pre-staging OS disks.
- From the drop-down lists, select the **Days** and **Times** the session host VMs' OS disks should be pre-staged.
- **Leave desktops that are not assigned to a user with STOPPED OS disk type:** Select this option so that desktop VMs that are unassigned to a user do not have the OS disk converted from STOPPED to RUNNING.
- **Use intelligent disk pre-staging for users:** Select this option to have intelligent disk pre-staging learn user behavior and automatically adjusts the disk pre-stage times.

Note: This feature requires AVD insights to be enabled and configured for the host pool.

- **Mode:** From the drop-down list, select the mode.

Note:

- **Hybrid Mode:** Disks are always be pre-staged based on the defined schedule. The behavior of users whose work patterns are learned, and additional staging activity are scheduled. This function is designed as "learning mode," with the benefits of both the standard pre-stage functionality and learned requirements.
- **Automated Mode:** Disks are pre-staged for existing users only according to the learned schedule. New users respect the defined schedule until Intelligent pre-staging has enough data to automate this process. Disks are pre-staged 30 minutes before anticipated user log on events.

6. Enter the following **Auto-Grow** information:

Note: Automatically add desktops to the host pool when the number of unassigned desktops remaining falls below a specified threshold.

- **Auto-Grow:** Toggle this option on to enable auto-grow.
- **Add a new host when the number of available (not assigned to a user) falls below:** Type the threshold and from the drop-down list, select whether the threshold is a number of desktops or a percentage of total desktops.

7. Enter the following **Auto-Shrink** information:

Note: The system automatically remove desktops that have not been used in a long time.

- **Auto-Shrink:** Toggle this option on to enable auto-shrink.
- **Delete VM if the user hasn't logged in for:** Type the number of days to wait before the system automatically deletes the VM.

Note: User activity on this session host VM is determined based on Nerdio Manager auto-scale history and AVD diagnostics data. Each time the desktop is processed by auto-scale, an Azure tag with date/time the desktop was last used is set. If the desktop hasn't been used for the number of days specified in this setting, the session host VM is shut down and a "pending deletion" tag is set.

- **Desktop will be set to "Pending deletion" state and deleted after:** From the drop-down list, select the "Pending deletion" duration.

Note: The desktop is set to "Pending deletion" state by the auto-scale process by adding a tag to the VM. A task is logged during this process, which can be used for admin notification of a desktop entering the "Pending deletion" state. There also are notification banners in the Nerdio Manager UI indicating that a personal host pool has VMs that are pending deletion. After the "pending deletion" period expires (default: 24 hours), the VM is permanently deleted.

- **Exclude the following groups (or individual users):** Enable this option, and then select the group(s) or individual user(s) to exclude from auto-shrink.

Note: Desktops assigned to users listed here are **not** automatically removed, even after a prolonged time of inactivity.

- **Exclude unassigned Desktops from Auto-shrink:** Select this option to exclude desktops that have not been assigned to a user from the auto-shrink operations.

Note: Use this setting in combination with Auto-Grow to maintain a buffer of free unassigned desktops.

- **Scripted actions to run when a host is scheduled to shrink:** From the drop-down list, select the scripted action(s) to run after the VM is marked to auto-shrink.
- **Notify users of scheduled deletion:** Select this option to notify the user via email about deletion of their desktop when the inactivity period is exceeded.

Note: Notifications on the **Settings > Nerdio environment** page must be enabled for this feature to work.

- **Message Subject:** Expand this option to type the subject line of the auto-shrink message.
- **Message Text:** Expand this option to open the editor to create a custom auto-shrink message for users.

Note: The following variables are available for use in the message body:

- **%HOSTPOOL%:** Returns the name of the affected host pool.
 - **%HOSTNAME%:** Returns the specific host name.
 - **%HOST_IDLE_DAYS_THRESHOLD%:** Returns the configured maximum idle days before auto shrink is started.
 - **%SHRINK_TIME_UTC%:** Returns the exact time in UTC when the auto-shrink task is set to occur.
 - **%SHRINK_DATE%:** Returns the exact date when the auto-shrink task is set to occur.
 - **%SHRINK_DATE_EUR%:** Returns the exact date when the auto-shrink task is set to occur in dd/MM/YYYY (European) format.
 - **%IMAGE_NAME%:** Returns the VM's image name.
 - **%FRIENDLY_WORKSPACE_NAME%:** Returns the workspace's friendly name.
 - **%FRIENDLY_HOSTPOOL_NAME%:** Returns the host pool's friendly name.
 - **%VM_SIZE%:** Returns the VM's size.
 - **%DISK_SKU%:** Returns the VM's disk SKU.
 - **%USER_NAME%:** Returns the name of the user logged in to the VM.
-
- **Notify an additional email recipient when desktops are scheduled to be deleted:** Select this option to notify an additional email recipient when desktops are scheduled to be deleted.
 - **Send notification emails to:** Type the additional recipient's email address.
 - **Send notification emails from:** Type the sender's email address.

- **Notifications frequency (Premium only):** From the drop-down list, select how frequently the email reminders are sent to the user.

Note: A final email is always be sent 1 day before the scheduled deletion.

8. Enter the following **Auto-Heal Broken Hosts** information:

Note: Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts:** Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is:** From the drop-down lists, select the desired statuses along with the session status.

Note: The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft [article](#) for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

- **Minutes before first action:** Type the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

Notes:

- You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
 - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.
- **Minutes between recovery actions:** Type the number of minutes to wait after each recovery action step before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

Note: If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

9. Once you have entered all the desired information, select **Save** or **Save & close**.

To enable schedule-based personal host pool auto-scaling:

1. **Auto-scale Mode:** From the drop-down list, select the **Schedule-based**.
2. Enter the following **Host Pool Properties** information:
 - **Start on connect:** Select this option to start the desktop on connect.
3. Enter the following **Working Hours** information:
 - From the drop-down lists, select the **Days** and **Times** the session host VMs' OS disks should be pre-staged.
 - **Power off aggressiveness:** From the drop-down list, select the power off aggressiveness. (Schedule-based only)

Note:

- **High:** Power off all session host VMs, including those with active and disconnected sessions. Users with active sessions are sent a message, defined below, and given time to sign out before their session host VM is powered off.
 - **Medium:** Power off only those session host VMs that do not have an active user session, including those with disconnected sessions.
 - **Low:** Only power off those session host VMs that have no active or disconnected sessions.
- **Power on timing:** From the drop-down list, select the power on timing. (Schedule-based only)

Note:

- **Never:** Do not power on session host VMs at the beginning of the working hours defined above. Users must manually power on their session host VMs.
 - **Once:** All sessions host VMs are only powered on once at the start of the working hours. If a session host VM is powered off after the start of the working hours, it is not automatically powered back on by auto-scale.
 - **Continuously:** All session host VMs are powered on at the start of the working hours. In addition, for the duration of the working hours, auto-scale automatically powers on any session host VMs that were manually powered off.
- **Power off timing:** From the drop-down list, select the power off timing.

Note:

- **Never:** Do not power off session host VMs at the end of the working hours defined above.
 - **Once:** At the end of the working hours, all session host VMs are powered off, subject to the aggressiveness defined above. If any session host VMs are manually powered on outside of the working hours, auto-scale does not automatically power them off.
 - **Continuously:** At the end of the working hours, all session host VMs are powered off, subject to the aggressiveness defined above. If any session host VMs are manually powered on outside of the working hours, auto-scale automatically powers them off, subject to the aggressiveness defined above.
- **Include hosts without assigned user:** Select this option to also start unassigned desktops during the auto-scale process.

Note: This may be useful for organizations wishing to perform scheduled tasks against desktops during the working day.

4. Enter the following **Host OS Disks** information:

- **Set all hosts to running OS disk type during work hours:** Select this option to convert all stopped host VM OS disks to running disk type during the working hours defined above.

Note: This is necessary to ensure that if a VM is started via Azure Start VM on Connect that it has the correct, high-performance disk type. When this setting is enabled, all "Disk type differs from policy" warnings are hidden for this pool.

- **Use intelligent disk pre-staging for users:** Select this option to have intelligent disk pre-staging learn user behavior and automatically adjusts the disk pre-stage times.

Note: This feature requires AVD insights to be enabled and configured for the host pool.

- **Mode:** From the drop-down list, select the mode.

Note:

- **Hybrid Mode:** Disks are always be pre-staged based on the defined schedule. The behavior of users whose work patterns are learned, and additional staging activity are scheduled. This function is designed as "learning mode," with the benefits of both the standard pre-stage functionality and learned requirements.
- **Automated Mode:** Disks are pre-staged for existing users only according to the learned schedule. New users respect the defined schedule until Intelligent pre-staging has enough data to automate this process. Disks are pre-staged 30 minutes before anticipated user log on events.

5. Enter the following **Auto-Grow** information:

Note: Automatically add desktops to the host pool when the number of unassigned desktops remaining falls below a specified threshold.

- **Auto-Grow:** Toggle this option on to enable auto-grow.
- **Add a new host when the number of available (not assigned to a user) falls below:** Type the threshold and from the drop-down list, select whether the threshold is a number of desktops or a percentage of total desktops.

6. Enter the following **Auto-Shrink** information:

Note: The system automatically remove desktops that have not been used in a long time.

- **Auto-Shrink:** Toggle this option on to enable auto-shrink.
- **Delete VM if the user hasn't logged in for:** Type the number of days to wait before the system automatically deletes the VM.

Note: User activity on this session host VM is determined based on Nerdio Manager auto-scale history and AVD diagnostics data. Each time the desktop is processed by auto-scale, an Azure tag with date/time the desktop was last used is set. If the desktop hasn't been used for the number of days specified in this setting, the session host VM is shut down and a "pending deletion" tag is set.

- **Desktop will be set to "Pending deletion" state and deleted after:** From the drop-down list, select the "Pending deletion" duration.

Note: The desktop is set to "Pending deletion" state by the auto-scale process by adding a tag to the VM. A task is logged during this process, which can be used for admin notification of a desktop entering the "Pending deletion" state. There also are notification banners in the Nerdio Manager UI indicating that a personal host pool has VMs that are pending deletion. After the "pending deletion" period expires (default: 24 hours), the VM is permanently deleted.

- **Exclude the following groups (or individual users):** Enable this option, and then select the group(s) or individual user(s) to exclude from auto-shrink.

Note: Desktops assigned to users listed here are **not** automatically removed, even after a prolonged time of inactivity.

- **Notify user when their desktop is about to be deleted:** Select this option to notify the user via email about deletion of their desktop when the inactivity period is

exceeded.

Note: Notifications on the **Settings > Nerdio environment** page must be enabled for this feature to work.

- **Message Subject:** Expand this option to type the subject line of the auto-shrink message.
- **Message Text:** Expand this option to open the editor to create a custom auto-shrink message for users.

Note: The following variables are available for use in the message body:

- **%HOSTPOOL%:** Returns the name of the affected host pool.
 - **%HOSTNAME%:** Returns the specific host name.
 - **%HOST_IDLE_DAYS_THRESHOLD%:** Returns the configured maximum idle days before auto shrink is started.
 - **%SHRINK_TIME_UTC%:** Returns the exact time in UTC when the auto-shrink task is set to occur.
 - **%SHRINK_DATE%:** Returns the exact date when the auto-shrink task is set to occur.
-
- **Notify an additional email recipient when desktops are scheduled to be deleted:** Select this option to notify additional users about auto-shrink activity.
 - **Send notification emails to:** Type the additional email addresses.
 - **Send notification emails from:** From the drop-down list, select the "Send From" email address.

7. Enter the following **Messaging** information:

Note: The system sends messages to any users connected to a session host that has been selected for scale in.

- **Send a warning message to active users:** From the drop-down list, select the number of minutes before scaling in that the message should be sent.
- **The message should say:** Type the warning message text.

8. Enter the following **Auto-Heal Broken Hosts** information:

Note: Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts:** Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is:** From the drop-down lists, select the desired statuses along with the session status.

Note: The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft [article](#) for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

- **Minutes before first action:** Type the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

Notes:

- You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
 - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.
- **Minutes between recovery actions:** Type the number of minutes to wait after each recovery action step before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

Note: If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

9. Once you have entered all the desired information, select **Save** or **Save & close**.

Related Topics

"Create Dynamic Host Pools" on page 214

"Enable Dynamic Host Pool Auto-scaling" on page 219

Auto-scale: Cost Optimization Session Host VM OS Disk Storage

There are two types of costs associated with a VM - compute costs and storage costs. Compute costs are incurred only when the VM is in use, while the storage costs are incurred even when the VM is stopped.

The **Running OS disk size** and **Stopped OS disk type** settings, along with other auto-scale settings, provide up to 75% storage cost savings. The auto-scale logic can automatically change

the OS disk type of VMs in both pooled and personal host pools to a cheaper storage tier (from premium SSD to standard HDD), while the host VM is powered off, and back to the higher performance tier immediately before it is started.

To configure Running OS disk size and Stopped OS disk type settings on your session hosts:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Auto-scale > Configure**.
3. In the **Auto-Scale** section, configure the following:
 - **Running OS Disk (Template)**: From the drop-down list, select the running disk type.
 - **Stopped OS Disk Type**: From the drop-down list, select the stopped disk type.
4. Once you have changed the parameters above, select **Save & close**.

Note: With Azure's **Start VM on connect** feature, VMs can be powered on outside of Nerdio Manager and may override **Running OS disk size** and **Stopped OS disk type**. That is, a VM powered on by the **Start VM on connect** feature is not able to change the disk performance. Instead, we recommend configuring **Pre-stage** to enable "Set all hosts to running os disk type" if **Start VM on connect** is enabled with storage scaling.

Directory	FRIENDLY NAME:	AADJ Multi-session Desktop
AVD	DESCRIPTION:	
VM Deployment	LOAD BALANCING: ⓘ	
Custom RDP	<input type="radio"/> Breadth first ⓘ	
FSLogix	<input checked="" type="radio"/> Depth first ⓘ	2
Azure Monitor		Session limit ⓘ
Sepago	<input type="checkbox"/> Validation environment ⓘ	
Session time limits	<input checked="" type="checkbox"/> Allow end-users to manually start a session host when none are started ⓘ	
Disaster Recovery	<input checked="" type="checkbox"/> Start VM on connect ⓘ	

For a single-user host pool that has schedule-based auto-scaling, you can configure the **Host OS Disks** in and out of working hours. For example, you can specify Premium SSD when the VM is running and Standard SSD when the VM is stopped, thus saving on Azure storage costs

To configure Host OS disks:

1. Navigate to **Workspaces > Dynamic host pools**.
2. Locate the single-user host pool you wish to change.
3. From the action menu, select **Auto-scale > Configure**.
4. In the **Host OS Disks** section, configure the following:
 - **Running**: From the drop-down list, select the disk type when the VM is running.
 - **Stopped**: From the drop-down list, select the disk type when the VM is stopped.
5. Once you have changed the parameters above, select **Save & close**.

For a multi-user host pool that has its **Minimum Active Host Capacity** set to 0, you can configure the system so that all stopped VM OS disks are automatically converted to **Running OS Disk** type during the pre-staging hours. This is necessary to ensure that if a VM is started via **Azure Start VM on Connect** that it has the proper high-performance disk type.

To configure the pre-staging OS disk type conversion:

1. Locate the single-user host pool you wish to work with.
2. From the action menu, select **Auto-scale > Configure**.
3. In the **Pre-stage Hosts** section, configure the following:
 - If necessary, enable **Pre-stage hosts**.
 - **Set all host to running OS disk type**: Select this option.

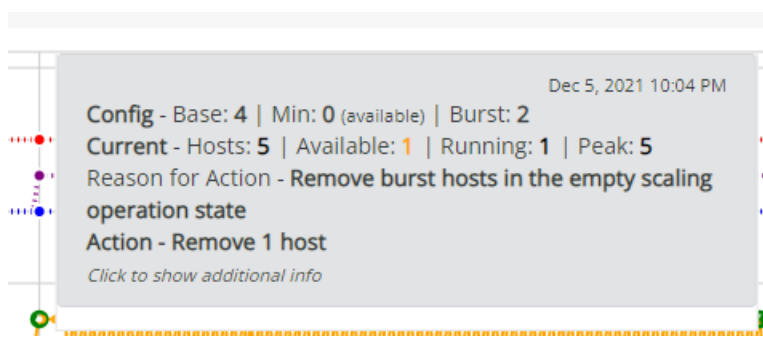
- Set the pre-stage time as desired.
4. Once you have entered all the desired information, select **Save & close**.


Auto-scale History for Dynamic Host Pools




The auto-scale history visualization helps you understand auto-scale behavior and how it impacts your deployment.

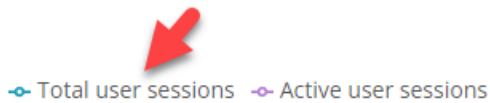
The following are important auto-scale history features.

- **Time Range:** At the top of the window, select the desired time range to display.
- **Show:** At the top of the window, select the desired graph(s) to display.
- **Savings:** At the top of the window, you can view auto-scale savings. Select **view details** to see the savings details.
- **Zoom In:** For the **Active users** graph only, click and drag the mouse over the section of the graph you wish to zoom in on. When you are zoomed in, select **Zoom-out** to restore the full graph.
- **Gray Background:** A gray background on a graph indicates that a scale-in restriction is active during that time period.
- **Hover:** You can hover over any part of any graph to see its details. For example:



- **Action Points:**
 -  **Scale Out:** This action point indicates that a scale-out event took place. (Red indicates that the scale-out event is costing money.)

-  **Scale In:** This action point indicates that a scale-in event took place. (Green means that the scale-in event is saving money.)
 -  **Auto-Heal:** This action point indicates that an auto-heal event took place.
 -  **Azure Issue:** This indicates that there was a problem communicating with Azure. If this occurs frequently, please contact Nerdio Manager technical support.
- At the bottom of any graph, select the data set name to toggle on/off the display line associated with that information. For example, select **Total user sessions** to suppress that line on the graph. Select it again to display it.



- Depending on which auto-scale trigger has been configured, that determines which graph contains extra values. For example, if the auto-scale trigger is configured based on CPU Usage%, then the CPU Usage% graph contains extra data sets such as Scale In Threshold and Scale Out Threshold.

Note: Regardless of which auto-scale trigger is configured for the host pool, you can configure the host pool to always have the auto-scale process collect CPU, RAM, and Average active sessions data. See "Host Pool AVD Configuration" on page 277 for details. Otherwise, the auto-scale process only collects data related to the auto-scale trigger.

To view auto-scale history for a dynamic host pool:

1. Locate the dynamic host pool you want to work with.
2. From the action menu, select **Auto-scale > History**.
3. Select the desired time range and the specific graphs to display.
 - **Active hosts:** The Active hosts graph displays **Section 1** of the auto-scale configuration (Host Pool Sizing) and host pool activity as recorded by the auto-scale process. This includes the following:

- **Base capacity:** This is the number of session host VMs to always be part of this host pool. These session hosts may be stopped or running.
- **Min active capacity:** This is the minimum number of running session hosts that are always available.
- **Burst capacity:** This is the capacity to burst above the base capacity of session host VMs when there is user demand. The system automatically creates up to this number of new session host VMs above the base capacity when needed.
- **Active hosts:** The current number of active session hosts at this point in time.
- **Peak capacity:** This the highest number of recorded session hosts for this time period.

Notes:

- Select an action point to see its details in the **Related Tasks** section at the bottom of the window. In addition, for any task shown in Related Tasks, select **Details** to view the task's details.
 - Select any point on the graph to see the status of the session hosts in the **Hosts Snapshot** section at the bottom of the window.
- **User sessions:** The User sessions graph displays the following information about when users are signing in and signing out. This includes users connected to full desktop sessions or RemoteApps.
 - **Total user sessions:** The total number user sessions, which includes disconnected sessions.
 - **Active user sessions:** The total number of active user sessions, which only includes users who are actively connected.
 - **CPU usage %:** The CPU usage% graph displays the Average CPU%.
 - **RAM usage %:** The RAM usage% graph displays the Average RAM%.

- **Average user sessions:** The Average user sessions displays the average number of user sessions per session host.

Note: If CPU usage%, RAM usage%, or Average user sessions is the auto-scale trigger, then additional scale-out and scale-in data sets are displayed on the graph.

- **Savings (graph):** The Savings graph displays compute and storage savings.

Note: As session hosts are started or created, the savings goes down due to increased compute and storage resources. As session hosts are shut down, removed, or disk types converted, the savings go up.

Auto-scale Session Host Scale In-Out Restrictions

Individual session host VMs within host pools with auto-scale enabled can be excluded from scale in and/or scale out indefinitely, or for a predefined period. This is especially useful when certain session host VMs are not healthy and need to be put into maintenance mode or when long running operations must not be interrupted during a scale in window.

To restrict scale in or scale out for a session host:

1. Locate the session host you wish to work with.
2. From the action menu, select **Restrict scale in**.
3. Enter the following information:
 - **Would you like to exclude...:** From the drop-down menu, select the type of exclusion.
 - **Exclusion Duration:** Select either an indefinite exclusion or select a date and time when the exclusion ends.
4. Once you have made the desired selections, select **Confirm**.

Note: The scale in restrictions take effect once the task completes. You can see the task's progress in the **Host Pool Tasks**.

Add a New Session Host to a Dynamic Host Pool

Once a host pool is created, you can manually add session hosts.

Tip: When using Dynamic Host pools it is recommended that you create the hosts with auto-scaling configured. See "Enable Dynamic Host Pool Auto-scaling" on page 219 for more information.

To add a session host to a dynamic host pool:

1. Locate the dynamic host pool you wish to work with.
2. From action menu, select **Hosts > Add new**.
3. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 86 for details.

- **Run now or Schedule:** Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **Save**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
- **Host Count:** Type the number of session hosts to add to the host pool during creation.
- **Host Name:** Type the name of the newly added hosts for the Exact name, a Prefix or the Prefix+Pattern.
 - **Exact/Prefix/Pattern:** From the drop-down list, select whether to use an Exact name, a Prefix, or a Pattern.

Note:

- **Exact** applies when adding a single host and specifying an exact name. For example, MYADVHOST.
 - **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
 - **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
 - Example 1: AVDHOST{####} (AVDHOST000..AVDHOST999).
 - Example 2: AVDHOST-{????} (AVDHOST-d83, AVDHOST-7sl, etc.).
- **Network:** From the drop-down list, select the network. The network determines the Azure region of the VM.
 - **Desktop Image:** From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.

Note: The **Unmanaged Azure Compute Gallery image versions** section is at the bottom of the list. These are unmanaged, backup versions of images that were created while activating staged images. These images can be used to restore any changes made to session hosts.

- **VM Size:** From the drop-down, select the VM type for newly created session hosts.
- **OS Disk:** From the drop-down list, select the OS Disk type and size for newly created session hosts.

Note: This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S-type) is not recommended. Premium SSD provides best performance.

- **Resource Group:** From the drop-down list, select the resource group to contain the VMs.
- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the session host.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

- When **Host Count** is greater than 1, enter the following:
 - **Process Host in Groups Of:** Type the number of concurrent operations when adding the new hosts.
 - **Number of failures before aborting:** Type the number of failed tasks before the process stops.
 - **Schedule:** If scheduled, enter the schedule information to run this job per the schedule.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Host Pool Disaster Recovery

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

Notes:

- This feature is only available in the Nerdio Manager **Premium** edition.
- This feature does not support **Single user desktop (personal)** host pools.

The disaster recovery feature in Nerdio Manager automatically distributes newly created VMs between a primary and secondary Azure region. When the users connect, they are evenly split between the two regions. In case of an outage in one of the regions, users are automatically connected to the remaining region.

The networking in both regions must be configured to communicate with the Active Directory domain controllers (or for the future Entra ID). Currently, in production scenarios, you need line of sight to the Active Directory domain controllers from networks in both locations.

The active-active DR setup is configured on the host pool level. It distributes the VMs, takes care of the FSLogix configuration, and replication of the profiles. The FSLogix profiles are replicated between storage locations in both regions, leveraging the FSLogix Cloud Cache feature.

Prerequisites: A network with line of sight visibility for domain controllers in both regions and an Azure files storage location for the FSLogix local profile copies.

Note: To enable DR on this host pool, the selected FSLogix profile must use Cloud Cache. Create a new profile, or modify an existing one, with Cloud Cache enabled and select it on the FSLogix properties page.

Both primary and secondary FSLogix storage locations are configured on every new session host with Cloud Cache replication. VMs in the primary Azure region are configured with FSLogix storage in that region as primary and VMs in the secondary Azure region are configured with FSLogix storage in that region as primary.

If there are existing hosts in the host pool, delete and recreate them after enabling DR.

To configure host pool disaster recovery:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > Disaster Recovery**.
3. Enter the following information:
 - **Enable Disaster Recovery:** Toggle this option on.
 - **Secondary VM Prefix:** Type the prefix to be used when creating session hosts in the secondary Azure region.

Note: The Name prefix limit is 10 valid, Windows computer name characters. When using a prefix, the system automatically appends “-xxxx” to the name prefix to make a unique name. Do not add “-“ to your name prefix.

- **Secondary Network:** From the drop-down list, select a secondary network that 50% of the newly created VMs are connected to. The selected network also determines the Azure region of the VM.
- **Secondary Resource Group:** From the drop-down list, select the resource group that contains the VMs in the secondary region.
- **Desktop Image (Template):** From the drop-down list, select the desktop image that is used for newly created VMs in the primary and secondary regions.

Note: The image must be stored in the Azure Compute Gallery and replicated to both regions.

- **Secondary FSLogix Storage:** From the drop-down list, select the FSLogix storage location in the secondary region.
 - **Secondary FSLogix Office Container:** From the drop-down list, select the FSLogix office container location in the secondary region.
4. Once you have entered all the desired information, select **Save** or **Save & close**.

You now need to review the host pool's auto-scale configuration.

5. Locate the host pool.
6. From the action menu, select **Auto-scale > Configure**.
7. Make sure that the **Desktop Image (Template)** is the same that was configured in disaster recovery.
8. In the **Host Pool Sizing** section, enter the **Base host pool capacity**.
9. Select **Save & close**.

Related Topics

"FSLogix settings and configuration" on page 162

Host Pool Backup

Nerdio Manager allows you to enable automatic Azure backup of pooled and personal host pools.

To configure host pool backups:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > Backup**.
3. Enter the following information:
 - **Enable backup:** Toggle this option on.
 - **Disable backups on VMs that were previously protected by Nerdio Manager:** Select this option to stop all VM backups that were created by Nerdio Manager. If not selected, existing protected items are not affected.
 - **Vault:** Create a new vault, or select an existing vault, to contain the backups for this host pool.

Note: The vault must be in the same region as the VMs. Backup for VMs that are not in the same region as the vault are skipped.

- **Policy:** Create a new backup policy, or select an existing backup policy, for this host pool.

Note: The backup policy dictates the frequency and retention of backups. The higher the frequency, and the longer the retention, results in higher costs.

- **Backup schedule:** Enter the following schedule information:
 - **Frequency:** From the drop-down list, select the frequency.
 - **Time and Timezone:** From the drop-down lists, select the time and timezone to run the backup.
 - **Days:** For weekly backups, select the day(s) to run the backup.
 - **Retention range:** Enter the following retention information:
 - **Instant recovery snapshots retention days:** Type the number of days to retain the instant recovery snapshots.
 - **Retention of daily/weekly backup point:** Type the number of days/weeks to retain the daily backup point.
 - **Retention of weekly backup point:** For daily backups, from the drop-down list, select the day(s) to retain a weekly backup point. In addition, specify the number of weeks.
 - **Retention of monthly backup point:** Select this option to retain a monthly backup point.
 - Configure the monthly backup point, as desired.
 - **Retention of yearly backup point:** Select this option to retain a yearly backup point.
 - Configure the yearly backup point, as desired.
4. Once you have entered all the desired information, select **Save** or **Save & close**.

Clone host pools and host pool settings


Nerdio Manager allows you to clone existing host pools or just the host pool settings that can then be applied to other host pools.

Clone host pools

If you clone a host pool, this creates a new host pool based on an existing one, cloning all its customizations. Therefore, there is no need to reconfigure the environment from scratch.

The clone feature allows you to create several template host pools. These configurations contain no actual hosts and provide no desktops to users, but they provide setups for the future host pools and their environments. You can clone them according to your requirements when you need to deploy new capacity.

To clone a host pool:

1. Locate the host pool you wish to clone.
2.
 - **Classic UI:** From the action menu, select **Clone host pool**.
 - **New UI:** Select the more options  menu, and select **Clone host pool**.
3. Enter the following information:
 - **Destination Workspace:** From the drop-down list, select the workspace you want to use.
 - **Resource Group:** From the drop-down list, select the resource group to contain the VMs.
 - **New Host Pool Name:** Type the host pool's name.
 - **Friendly Name:** Type the friendly name that is visible to end users.
 - **Description:** Type the description visible to admins.
 - **New Host Name Prefix:** Type the unique prefix for the VMs to be used when creating multiple session hosts.

Note: This must not be the same as any existing host pools. The name prefix limit is 10 valid, Windows computer name characters. When using a prefix, the system automatically appends “-xxxx” to the name prefix to make a unique name. Do not add “-“ to the name prefix.

- **Copy users and group assignments:** Select this option to copy the users and groups assigned to this host pool and paste them into the clone.
 - **Use new Custom app group names:** Select this option to specify a new custom app group name.
 - **Custom App Group Name:** Type the new custom app group name(s).
4. When you have entered all the desired information, select **Clone**.

A copy of the existing host is generated with a different name and a different VM prefix. The new cloned host pool is added to the list of the existing host pools.


Note: By default, the auto-scale option for this host pool is off. Do not forget to turn it on. See "Enable Dynamic Host Pool Auto-scaling" on page 219 for details.

Tip: To delete the existing host pool, refer to Delete Hosts, Host Pools, and Workspaces.

Clone host pool settings

If you clone host pool settings, this allows you to apply just the settings of the selected host pool, and apply them to another host pool.

To clone host pool settings:

1. Locate the host pool you wish to clone the settings from.
2.
 - **Classic UI:** From the action menu, select **Apply to other host pools**.
 - **New UI:** Select the more options  menu, and select **Apply to other host pools**.
3. From the drop-down list, select the destination host pool. This is the host pool to which you want to apply the pool settings to.

Note: The list of available host pools is filtered based on the source host pool. Only host pools of the same type - Static, Dynamic, or Hybrid - are shown.

4. Select **Save**.

Related Topics

"Host Pools" on page 204

Bulk Host Actions

You can perform bulk actions on all the session hosts, or on selected sessions hosts, in a host pool.

Note: Many of the tasks listed below can be run by scheduling the task. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.

To perform a bulk host action on all session hosts:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Manage Hosts**.
3. Select one of the following bulk actions:
 - **Add New:** Add a new session host the host pool. See "Add a New Session Host to a Dynamic Host Pool" on page 258 and "Add a New Session Host to a Static Host Pool" on

page 212 for details.

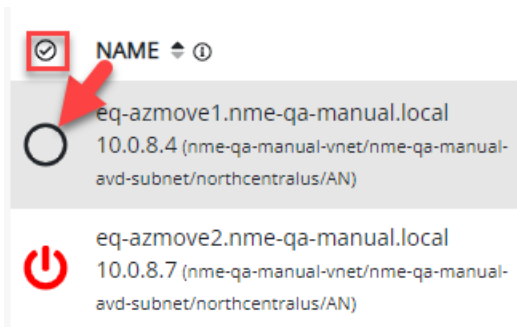
- **Re-size/Re-image:** See "Resize/Re-image a Host Pool" on page 270 for details.
- **Restart:** See "Restart a Host Pool" on page 273 for details.
- **Power on:** Power on all the hosts.
- **Power off:** See "Power Off a Host Pool" on page 274 for details.
- **Request logs:** Download the selected logs to a zip file.
- **Exclude from auto-scale:** Exclude all the hosts from auto-scale.
- **Activate:** Take all the hosts out of drain mode.
- **Deactivate:** Put all the hosts into drain mode.
- **Delete all:** See Delete Hosts, Host Pools, and Workspaces for details.
- **Message Users:** Send notifications to all the users connected to all the hosts in the host pool.
- **Disconnect Users:** Disconnect all users from all session hosts.
- **Log off users:** Sign out all users from all session hosts.
- **Run script:** Run a PowerShell command on all the hosts in the host pool. See "Run Bulk Host Scripted Actions" on page 287 for details.
- **Exclude from auto- scale selected:** See "Auto- scale Session Host Scale In- Out Restrictions" on page 257 for details.

Note: Some bulk actions noted above allow you to perform the action in groups. You need to enter the following:

- **Process Host in Groups Of:** Type the number of concurrent operations for the bulk action.
- **Number of failures before aborting:** Type the number of failed tasks before the process stops.

To perform a bulk action on selected session hosts:

1. Locate the host pool you wish to work with.
2. Select the host pool's **Name** to view all the session hosts in the host pool.
3. In the list of session hosts, select the one(s) you want to work with by selecting them in the column.



4. Once you have selected all the desired session hosts, select **Select bulk action**, and then select any of the relevant actions that apply to the session hosts.

Note: For example, you have 5 session hosts in the host pool, with 3 powered on and 2 powered off. The action menu displays (this is a partial list of relevant actions):

- **Power off selected (3)**
- **Power on selected (2)**
- **Restart selected (3)**

That is, only the 3 session hosts that are powered on can be powered off or restarted. Only the 2 session hosts that are powered off can be powered on.

Related Topics

"Run Bulk Host Scripted Actions" on page 287

Delete Hosts, Host Pools, and Workspaces

"Host Pools" on page 204

"Convert a Static Host Pool to Dynamic" on page 211

Resize/Re-image a Host Pool

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

The system automates the process of updating the session hosts when there are changes that need to be made to applications, operating systems, or other system components. This is accomplished by use of desktop images.

You can use the updated image to:

- Re-image existing session hosts. (A common use case.)
- Create new session hosts.

In Nerdio Manager, the desktop image consists of the following Azure objects:

- A virtual machine that is used to manage the image.
- The actual image that is used to deploy session hosts.

Note: When you power on a desktop image, you are powering on the virtual machine.

To re-image session hosts with desktop images:

1. Navigate to **Desktop Images**.
2. Locate the desktop image you want to work with and power it on, if necessary.
3. Connect to the desktop using any remote connection tool (RDP) and make all the desired changes.
4. Once you have completed all the desired changes, return to the **Desktop Images**.
5. Select **Power off & set as image**.

6. When prompted to confirm your request, select **OK**.

Note: Once you confirm your request, an extensive automation process begins that commits the changes to an image object.

7. At the bottom of the **Desktop Images** window, in the **Desktop Images Tasks** section, you can see the task's progress. Select **Details** to see the task's details.
8. Locate the host pool you want to re-image.
9. From the action menu, select **Hosts > Resize/Re-image**.
10. Enter the following information:
 - **Run now or Schedule:** Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **OK**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Desktop Image:** From the drop-down list, select the desktop image you want to update the hosts with.
 - **VM Size:** Optionally, from the drop-down list select a new VM size.
 - **OS Disk:** Optionally, from the drop-down list select a new OS disk.
 - **Process Host in Groups Of:** Type the number of concurrent operations for the host re-imaging.

Warnings: A larger number of hosts selected allows the re-imaging process to complete quicker, but if there is an issue with the desktop image or Azure, many hosts may end up in an error state and unusable.

You must select this value with care. For example, if you have 150 hosts in the pool, you do not want to want to re-image them one at a time. That would take too long. On the other hand, you do not want to run all 150 operations at the same time. That could overload your environment. So, you may want to run 25 operations per group.

- **Number of failures before aborting:** Type the number of failed tasks before the process stops.

Note: This setting can help prevent a problem on the desktop image or Azure from making session hosts unavailable to the users.

- **After first group is done, set remaining hosts to drain mode:** Select this option to set all hosts that haven't yet been resized/re-imaged to drain mode as soon as the first group of hosts completes the resize/re-image process.

Note: This ensures that users who connect to their desktop are only directed to a host session VM that has already been resized/re-imaged.

- **Force Users to Log Off:** From the drop-down list, select the time to wait before forcing users to log off.

Note: You may force users to log off either immediately or after a specified time period. Optionally, by selecting **Never**, Nerdio Manager waits for all users to log off by themselves before re-imaging the host. That is, the re-imaging operation waits indefinitely until all users are logged off. If another scheduled re-imaging operation is due to run while it is waiting for the users to log off, the new scheduled task is skipped.

- **Set hosts to drain mode while waiting for users to log off:** Select this option to set the hosts to drain mode while waiting for all the users to log off.

Note: By default, this option is selected. You may only unselect it if **Force User to Log Off** is set to **Never**.

- **Send message while waiting for users to log off:** Select this option and type the text of the message to send.

11. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Restart a Host Pool

Nerdio Manager allows you to restart all session hosts in a host pool.

To restart all session hosts in a host pool:

1. Locate the host pool that contains the session hosts you want to restart.
2. From the action menu, select **Hosts > Restart**.
3. Enter the following information:
 - **Run now or Schedule:** Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **OK**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Log off users:** Select this option to sign out users before restarting.
 - **Process Host in Groups Of:** Type the number of restart operations that start at the same time.

Warning: You must select this value with care. For example, if you have 150 hosts in the pool, you do not want to restart them one at a time. That would take too long. On the other hand, you do not want to run all 150 restarts at the same time. That could overload your environment. So, you may want to run 25 restarts per group.

- **Number of failures before aborting:** Type the number of failed tasks before the process stops.
- **Messaging:** Optionally, toggle on messaging to send a message to all the users on a session prior to performing the operation.
 - **Delay:** From the list, select the time to send the message before the operation

starts.

- **Message:** Type the text of the message to send.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Power On a Host Pool

Nerdio Manager allows you to power on all session hosts in a host pool.

To power on all session hosts in a host pool:

1. Locate the host pool you want to power off.
2. From the action menu, select **Hosts > Power on**.
3. Enter the following information:
 - **Run now** or **Schedule:** Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **OK**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Restrict scale in for (hours):** Select this option to restrict auto-scale from scaling it in for the specified number of hours.
 - Type the number of hours for the auto-scale restriction.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Power Off a Host Pool

Nerdio Manager allows you to power off all session hosts in a host pool.

Note: If you are working with a dynamic host pool with auto-scaling enabled, if you power off all the session hosts, auto-scaling powers them back on again. If you need to power everything off, you must temporarily disable auto-scaling.

To power off all session hosts in a host pool:

1. Locate the host pool you want to power off.
 2. From the action menu, select **Hosts > Power off**.
 3. Enter the following information:
 - **Run now** or **Schedule**: Optionally, navigate to the **Schedule** tab to perform the power off operations during selected time frame(s). Otherwise, the power offs start as soon as you select **OK**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Log off users**: Select this option to sign out users before powering off.
 - **Restrict autoscale operations for (hours)**: Select this option to restrict auto-scale from scaling it in or out for the specified number of hours.
 - Type the number of hours for the auto-scale restriction.
 - **Process Host in Groups Of**: Type the number of power off operations that start at the same time.
-
- Warning:** You must select this value with care. For example, if you have 150 hosts in the pool, you do not want to want to power them off one at a time. That would take too long. On the other hand, you do not want to run all 150 operations at the same time. That could overload your environment. So, you may want to run 25 operations per group.
- **Number of failures before aborting**: Type the number of failed tasks before the process stops.
 - **Messaging**: Optionally, toggle on messaging to send a message to all the users on a session prior to performing the operation.
 - **Delay**: From the list, select the time to send the message before the operation starts.
 - **Message**: Type the text of the message to send.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Exclude Session Host VMs from Auto-scale During Power On/Off

Nerdio Manager allows you to disable auto-scale on a selected session host VM for a specified number of hours when manually powering the session host VM on or off.

In addition, when starting session host VMs on a schedule to apply updates, auto-scale does not automatically stop them until after the number of specified hours elapses. See "Power On a Host Pool" on page 274 and "Power Off a Host Pool" on page 274 for details.

To exclude Session Host VMs from auto-scale during power on/off:

1. Locate the session host VM that you wish to power on or off.
2. For a **Power On** request:
 - Select the option **Restrict scale in for (hours)**.
 - Type the number of hours for the auto-scale restriction.

Note: After session host VM is powered on, auto-scale does not scale it in for the specified number of hours.

3. For a **Power Off** request:
 - Select the option **Restrict autoscale operations for (hours)**.
 - Type the number of hours for the auto-scale restriction.

Note: After session host VM is powered off, auto-scale does not scale it in or out for the specified number of hours.

Host Pool AVD Configuration

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

Nerdio Manager enables you to customize the host pool's AVD settings.

To configure host pool AVD settings:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > AVD**.
3. Enter the following information:
 - **Friendly Name:** Type the friendly name that is visible to the end users.
 - **Description:** Type the description that is visible to the administrators.

Note: Both the Friendly Name and Description can be changed at any time.

- **Load Balancing:** Select the desired load balancing option.

Note: The load balancing algorithm is used by the AVD Management Service to determine how to route a particular user's desktop or RemoteApp connection.

Breadth First means that the load-balancing algorithm spreads the users evenly across all available session hosts.

Depth First means the load-balancing algorithm places all the users in the first session host until the host's session limit is reached. Only then, does it place the users in the next session host. If necessary, it powers on the VM and makes it available to the users.

- **Session Limit:** Type the number of sessions that a single host in the host pool can accept.
- **Validation environment:** Select this option designate this host pool as a validation host pool.

Note: Validation host pools receive service updates at a faster cadence than non-validation host pools, allowing you to test service changes before they are deployed broadly to production.

- **Allow the users to manually start a session host when none are started:** Select this option to allow a user to sign in to Nerdio Manager and perform service actions. For example, power on the session hosts within the host pool. Only specified users that have the permissions to sign in to Nerdio Manager can start the session host VM this way.
- **Start VM on connect:** The VM is powered on automatically when the user connects. Any user can start the VM when they sign in.
- **Unassign user from host pool when removing host:** For personal host pools, select this option to unassign the user from the host pool when the host is deleted.
- **Collect hosts CPU usage:** Select this option to have the auto-scale process always collect CPU usage regardless of the host pool's auto-scale trigger.
- **Collect hosts RAM usage:** Select this option to have the auto-scale process always collect RAM usage regardless of the host pool's auto-scale trigger.
- **Collect hosts average active sessions:** Select this option to have the auto-scale process always collect average active sessions data regardless of the host pool auto-scale trigger..
- **Enable Scheduled AVD Agent Update:** Toggle on this option to specify the day and time you want to update the AVD agent.

Note: Deploying updates at convenient times, or outside of peak business hours, ensures greater reliability and business continuity, while also enhancing the employee experience without interrupting business critical work.

- **Time Zone:** From the drop-down list, select the time zone for the scheduled update.

Note: Setting the time zone ensures that updates to the session host VMs in the host pool take place at the same time according to the selected time zone, regardless of the session host VMs' local time zones. See this Microsoft [article](#) for details.

- **Use local session host time zone:** Select this option to perform the agent update using the local time zone of each session host VM in the host pool.

Note: . Use this setting when all session host VMs in your host pool, or their assigned users, are in different time zones.

- **Maintenance window:** From the drop-down lists, specify the day and time for the agent update.

Note: All maintenance windows are two hours long.

- **Set additional maintenance window:** Optionally, select this option to specify a second maintenance window.

Note: Creating two maintenance windows gives the agent components an additional opportunity to update if the first update is unsuccessful.

- **Power on all hosts during window(s):** Optionally, select this option to power on all hosts in a pool during maintenance window operations to ensure the

installation of the latest AVD agent and other updates.

Note: Hosts that are started as part of this process are shut down after 2 hours. Hosts that were already running do not have their power state changed.

- **Exclude Drain mode hosts:** Optionally, select this option to exclude drain mode hosts from the AVD agent maintenance window tasks configured in the host pool properties.

4. Once you have entered all the desired information, select **Save** or **Save & close**.

Host pool VM deployment

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

Nerdio Manager enables you to customize the way session host VMs are deployed in a host pool. This is a feature-rich facility that is detailed below.

To configure host pool VM deployment:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > VM Deployment**.
3. Enter the following information:
 - **Set time zone:** Select this option, and from the drop-down list select the time zone, to set the time zone on the VM when it is provisioned.
 - **Enable time zone redirection:** Select this option to allow users to see their local device's time zone inside of their session.

- **Enable Accelerated Networking for VMs that support it:** Select this option to enable Accelerated Networking, if available.

Note: The Azure VM accelerated networking feature is available in some of the larger Azure VMs. This feature is useful for enterprise organizations and IT professionals who need to deploy, manage, and optimize large amounts of Azure Virtual Desktops. It speeds up networking performance of individual VMs.

If this feature is not supported on your Azure VM, it is not enabled. See this Microsoft [document](#) for more information.

- **Enable NVMe for VMs that support it:** Select this option to enable NVMe, if available.

Note: NVMe is a storage protocol that offers higher IOPs and throughput providing your workload with overall greater performance. See this Microsoft [document](#) for more information.

- **Install GPU drivers on supported VM sizes:** Select this option to install either [NVidia](#) or [AMD](#) drivers.

Note: GPU drivers can be installed on N-series VMs.

- **Distribute VMs across Availability Zones:** Select this option to automatically distribute newly created or re-imaged session host VMs across Availability Zones in the selected Azure region.

Note: See this Microsoft [article](#) for more details about Azure Regions and Availability Zones.

- **Place VMs on Dedicated Hosts:** Select this option to place the VMs to physical servers.

Note: See this Microsoft [article](#) for more details about Azure dedicated hosts.

- **Dedicated Host Group:** From the drop-down list, select the dedicated host group.
- **Dedicated Host:** From the drop-down list, select the dedicated host for the VMs.

Note: If **Automatic assignment** is selected, the VMs are automatically assigned to the appropriate hosts when powered on.

- **Place VMs in Capacity Reservation Groups:** Select this option to place the VMs in a capacity reservation group.

Note: See Manage Capacity Reservations Groups for full details.

- **Capacity Reservation Groups:** From the drop-down list, select the capacity reservation group(s).
- **Deallocate powered off but not deallocated VMs:** Select this option to have a periodic task check if any session host VMs are in a powered off (but not deallocated) state and automatically deallocate them to save on Azure compute costs.
- **Install App Attach certificates:** Select this option to install all stored certificates if the App Attach packages are added to this host pool.
- **Install Applications:** Select this option to install applications configured by recurrent UAM policies before moving the host out of drain mode.
- **Restart VM after deployment:** Select this option to restart the VM after it is created.

Note: If certain extensions are installed during deployment (FSLogix, Sepago, Virtual Desktop Optimizations, or User Sessions Time Limits), the VM is automatically rebooted even if this option is not selected.

- **Always prompt for password:** Select this option to always prompt the user for a password.

Note: This policy setting specifies whether Remote Desktop Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users signing in to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.

By default, Remote Desktop Services allows users to automatically sign in by entering a password in the Remote Desktop Connection client.

- If you select this option, users cannot automatically sign in to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They are prompted for a password to sign in.
 - If you do not select this option, users can always sign in to Remote Desktop Services automatically by supplying their passwords in the Remote Desktop Connection client.
- **Enable H.265 encoding on supported VM sizes:** Select this option to enable high efficiency video coding (H.265) hardware acceleration on VM sizes of N-series with NVIDIA GPU.

Note: Multimedia redirection isn't supported. Disable it on your session hosts by uninstalling the host component

- **Enable encryption at host:** Select this option so that data stored on the session host VMs is encrypted at rest and flows encrypted to the Storage service.

Notes:

- This setting only applies to newly created desktops.
 - Encryption sets are per subscription/region. You can create hosts in different subscriptions/regions, and based on the host's subscription/region we select the appropriate encryption set.
 - See this Microsoft [article](#) to learn more about the encryption at host feature.
- **Register:** If necessary, select this option to register the feature "microsoft.compute/encryptionathost" with the linked subscriptions that do not have this feature.

Notes:

- Nerdio Manager supports the use of both platform-managed keys (default) and customer-managed keys (Encryption Sets). If you are using Encryption Sets, these must be created in the same region as the target session host VMs.
- If this subscription was registered in Nerdio Manager using the "logged in user" option, you must use an account with Subscription Owner permissions to register these features.
- If this feature is not registered, hosts in the linked subscriptions would not have encrypted data.
- This is a sample pop-up warning message:

Some of linked subscriptions do not have registered feature "microsoft.compute/encryptionathost", so hosts in those subscriptions would be created without encryption.

You may solve this problem by clicking **register** links below.

Feature would be registered for selected subscription.


MPN-s150-Amol-01 260acb35-f90f-431e-ae50-006411c4c815 [register](#)

MFS Sponsored Subscription 73431ef6-cf54-4e50-a20f-1963e58970a4 [register](#)

Azure Gov Dev Subscription 3fdfe54b-cb3f-4fa8-a5fb-33e7e0d51b98 [register](#)

DataON e770f826-dc95-43e6-90f2-410bd14e34d5 [register](#)

Nerdio Data Analysis Subscription 274f113c-1199-4d20-ae3d-5a92c4d4011c [register](#)



- **Enable boot diagnostics:** Select this option to apply the Boot Diagnostics feature to desktops in this pool.

Note: This setting only applies to newly created desktops.

- **Storage accounts for boot data:** Optionality, from the drop-down list, select an available storage account to be used to store boot data.

Note: By default, Azure uses an automatic managed storage account for screen shots and other data. To use the default setting, leave this empty.

- **Enable watermarking:** Select this option to enable watermarking.

Note: Watermarking helps prevent sensitive information from being captured on client endpoints. When you enable watermarking, QR code watermarks appear as part of the remote desktops. The QR code contains the connection ID of a remote session that admins can use to trace the session.

- **Scale:** Select the scale, which is the size in pixels of each QR code dot. This value determines the number of squares per dot in the QR code.
- **Opacity:** Select the opacity, which is how transparent the watermark is, in percent, where 0 is fully transparent.
- **Width factor:** Select the width factor which determines the distance between the QR codes in percent. When combined with the height factor, a value of 0 would make the QR codes appear side-by-side and fill the entire screen.
- **Height factor:** Select the scale, which determines the distance between the QR codes in percent. When combined with the width factor, a value of 0 would make the QR codes appear side-by-side and fill the entire screen.
- **Enable Hibernation:** Select this option to save time and money by deallocating your virtual machine and saving the contents of its RAM to the root volume, allowing you

to resume from where you left off when your VM restarts.

- **Patch Orchestration Options:** From the drop-down list, select the patch orchestration option, which allows you to control how patches are applied to your virtual machine.
- **Security Type:** From the drop-down list, select the security type.

Note: Security type refers to the different security features available for a virtual machine. Security features like Trusted Launch and Confidential virtual machines improve the security of Gen2 VMs. However, additional security features have some limitations, which include not supporting back up, managed disks, and ephemeral OS disks.

- **Secure Boot:** Select this option to enable Secure Boot, which helps protect your VMs against boot kits, rootkits, and kernel-level malware.
- **vTPM:** Select this option to enable Virtual Trusted Platform Module (vTPM), which is TPM 2.0 compliant and validates your VM boot integrity apart from securely storing keys and secrets.
- **Integrity Monitoring:** Select this option to enable cryptographic attestation and verification of VM boot integrity along with monitoring alerts if the VM didn't boot because the attestation failed with the defined baseline.
- **Entra ID group(s):** From the drop-down list, select the default Entra ID group(s) to add the session hosts to.
- **Enforce Intune Compliance :** Select this option to make hosts unavailable to users until the Intune compliance requirements are met.

Note: You may select that all Intune policies are met or only compliance policies are met. In addition, enabling this feature may result in significant increase in provisioning time, depending on the configured Intune compliance requirements.

- **Allow non-admin users to shadow sessions:** Toggle on this option to enable selected non-admin users or groups to shadow sessions.

Note: Session shadowing is only available with multi-session versions of Windows OS. This feature does not work with Windows 10 Enterprise (single session).

- **User or Group Name:** From the drop-down list, select the users or groups to allow to shadow sessions.
- **Run scripted actions when...:** Toggle on the desired run script options.

For each option, enter the following information:

- **Script:** From the drop-down list, select the scripts to execute.

Note: You can select both Windows scripts and Azure Runbooks. In addition, you can drag and drop the scripts to change the order in which they are run.

- **Scripted actions input parameters:** If necessary, provide the required parameters.
- **Pass AD credentials:** Select this option to pass AD credentials.
- **AD Credentials:** From the drop-down list, select the AD credentials to pass.

4. Once you have entered all the desired information, select **Save** or **Save & close**.

Run Bulk Host Scripted Actions

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the [Azure PowerShell module issues report](#).

Nerdio Manager enables you to manage your environment using Scripted Actions, which are PowerShell scripts. By using Scripted Actions, you can perform bulk operations and automation to create and manage the AVD Environment using Nerdio Manager.

For more information about bulk host actions (in general), refer to "Bulk Host Actions" on page 267.

For example, you can take all of the session host VMs inside the host pool and install the latest version of Microsoft Teams and enable the AV redirection of the media optimizations for AVD.

To run a PowerShell script on all the hosts in a host pool:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Hosts > Run script**.

Note: See "Scripted Actions Overview" on page 173 for more information about creating and managing scripted actions.

3. Enter the following information:
 - **Run now** or **Schedule**: Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **OK**. See "Manage Schedules for Tasks" on page 91 for details about creating a schedule.
 - **Run the following scripted action**: From the drop-down list, select the script to run.
 - **Scripted actions input parameters**: If necessary, provide the required parameters.
 - **Pass AD credentials**: Select this option to pass AD credentials.
 - **AD Credentials**: From the drop-down list, select the AD credentials to pass.
 - **Restart VMs after scripted action**: Select this option to restart the VMs after script execution. It is preferable to use this option instead of using any PowerShell restart commands as Custom Script extension fails if the script restarts the computer.
 - **Exclude not running hosts**: Select this option to exclude stopped and deallocated hosts from scheduled scripted tasks to prevent additional resource costs being

incurred.

- **Process hosts in groups of:** Type the number of concurrent actions to execute during this bulk operation.
 - **Number of failures before aborting:** Type the number of failures that causes the process to stop.
 - **Messaging:** Toggle on the Messaging to send messages to active users.
 - **Delay:** From the drop-down list, select the number of minutes to wait after sending the message before starting the process.
 - **Message:** Type the message you want to send to the users.
4. Once you have entered all the desired information, select **Run now** (not scheduled) or **Save & close** (scheduled).

Note: If any session hosts VMs are currently powered off, they are automatically powered on and the command runs on these VMs. They are automatically powered off after the action ends.

Related Topics

"Bulk Host Actions" on page 267

Manage Host Pool User Assignments

Nerdio Manager allows you to view users assigned to various host pools. In addition, you can assign or unassign users from the host pool.

To manage host pool user assignments:

1. Locate the host pool you wish to work with.
2. In the **Status** column, select the number next to **Assigned Users** to view the users and groups.

DYNAMIC HOST POOLS (NME-QA-MANUAL-WORKSPACE1) ⓘ			
SEARCH		FILTER BY TYPE	
<input type="text" value="Search by name"/>		<input checked="" type="checkbox"/> Multi user desktop (pooled) (1) <input checked="" type="checkbox"/> Multi user RemoteApp (pooled) (0)	
NAME ⌵ ⓘ	FRIENDLY NAME ⌵ ⓘ	DESKTOP EXPERIENCE ⌵ ⓘ	STATUS ⓘ
AmolTest Testing new install (nme-qa-manual-rg)	AmolTest	Multi user desktop (pooled) Breadth first load balancing Max session limit: Unlimited (999,999)	User sessions: 0 Assigned users: 0 Assigned groups: 0 Hosts: 1 ON / 2 (CPUs: 4)
nme-qa-man-personalhp <no description> (nme-qa-manual-rg)	nme-qa-man-personalhp	Single user desktop (personal) Assignment Type: Direct	User sessions: 0 Assigned users: 10 Assigned groups: 0 Hosts: 0 ON / 6 (CPUs: 12)

- In the **Manage Assignments** window, you may search, sort, and filter the users and groups. For example, filter for all users not assigned to the host pool.
- To unassign users from the host pool, select the icon next to the user(s) you wish to unassign.

MANAGE ASSIGNMENTS FOR NME-QA-MAN-PERSONALHP ⓘ	
SEARCH	FILTER
<input type="text" value="Search for users or groups..."/>	<input checked="" type="radio"/> Show users (51191) <input checked="" type="radio"/> Show assigned (10) ⓘ <input type="radio"/> Show groups (73) <input type="radio"/> Show not assigned ⓘ <input type="radio"/> Show users and groups <input type="radio"/> Show assigned and not assigned ⓘ
NAME ⌵ ⓘ	EMAIL ⌵ ⓘ
<input checked="" type="checkbox"/> Aamos <input type="checkbox"/> Aamos <input checked="" type="checkbox"/> Besart <input checked="" type="checkbox"/> Besir M	<div style="background-color: #ccc; height: 100px; width: 100%;"></div>

- When you have selected all the users, select **Unassign**.
- To assign users to the host pool, select the icon next to the user(s) you wish to assign.
- When you have selected all the users, select **Assign**.

Apply Host Changes Without Re-Imaging

Nerdio Manager allows you to apply FSLogix changes to hosts without re-imaging.

Note: In legacy systems, the changes were applied only to newly created hosts. A message appears: **These changes will apply only to newly created (or re-imaged) hosts.**, because the changes apply during the VM creation. For more information refer to "FSLogix settings and configuration" on page 162.

To apply changes to a host without re-imaging it:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > FSLogix**.

Note: The same process applies to other third-party and user session time limits.

3. Select the option **Apply to existing hosts**.
4. Enter the following information:
 - **Process hosts in groups of:** Type the number of concurrent actions to execute during this bulk operation.
 - **Number of failures before aborting:** Type the number of failures that causes the process to stop.
 - **Messaging:** Toggle on the Messaging to send messages to active users.
 - **Delay:** From the drop-down list, select the number of minutes to wait after sending the message before starting the process.
 - **Message:** Type the message you want to send to the users.
5. Once you have entered all the desired information, select **Save** or **Save & close**.

- **Notes:**
 - This operation only adds new settings or updates the existing settings. No existing settings are deleted. To delete the existing settings, you must re-image the host pool. The re-imaging recreates the host and reapplies the settings from scratch.
 - Any powered off hosts are powered on and then powered off again when the process is complete.

Related Topics

"FSLogix settings and configuration" on page 162

Configure the Host Pool's Active Directory Settings

By default, every host pool uses the global default Active Directory configuration that was used when Nerdio Manager was installed. Nerdio Manager allows you to create multiple Active Directory profiles containing different service accounts and OUs, if required, We can then use these multiple profiles on different host pools.

To configure Active Directory for a host pool:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties > Directory**.
3. Enter the following information:
 - **AD Configuration:** From the drop-down list, select the Active Directory configuration.

For a **custom** configuration, enter the following:

- **Directory:** From the drop-down list, select the directory.
- **AD Domain:** Type the domain for session host VMs to join in Fully Qualified Domain Name (FQDN) format.
- **AD Username:** Type the username in FQDN format.

Note: This user must have permissions to create computer objects in the OU specified below and the ability to disable these AD computer objects when the VM leaves the AD domain.

- **AD Password:** Type the password.
- **Organization Unit:** Type the OU name in Distinguished Name (DN) format.

Note: This is the OU where all session host VMs and Desktop Images AD computer objects are created by default. Leaving this field blank places all the computer objects in the computer's AD container.

4. When you have entered all the desired information, select **Save** or **Save & close**.

Related Topics

"Entra ID - definition of terms" on page 16

"Configure Entra Domain Services for use with AVD" on page 21

Start VM on Connect for Pooled Host Pools

Nerdio Manager allows you to take advantage of the "Start VM on connect" feature. This feature powers on a session host VM in a host pool where all the session host VMs currently powered off. Therefore, if the user signs in, a VM is powered on to give this user a session.

Note: End users can start a session host VM in more than one way. It depends on the user's permissions.

- **Allow the users to manually start a session host when none are started:** This allows user to sign in to Nerdio Manager and perform service actions. For example, power on the session hosts within the host pool. Only specified users that have the permissions to sign in to Nerdio Manager can start the session host VM this way.
- **Start VM on connect:** The VM is powered on automatically when the user connects. Any user can start the VM when they sign in.

To configure Start VM on connect for pooled host pools:

1. Locate the host pool you wish to work with.
2. From the menu, select **Properties > AVD**.
3. Select the **Start VM on connect** option.
4. Select **Save** or **Save & close**.

Configure User Session Time Limits

Nerdio Manager allows you to apply host session limits to individual host pools at the host pool level. This enables you to:

- Optimize your AVD deployment and auto-scaling.
- Conserve resources by signing out users who leave their sessions open or leave themselves in a disconnected state.

Note:

- By default, the session time limits option is disabled. Session time limits do not apply, and the system accepts any changes that users make to a single image or through the group policy.
- Nerdio Manager applies session time limits through local policy changes on the session host VM. Session states are managed by the Windows OS rather than Nerdio Manager.

To set the user session time limits for full desktops:

1. Locate the host pool you want to work with.
2. From the action menu, select **Properties > Session time limits**.
3. Enter the following information:
 - **Enable user session time limits:** Toggle this option **On**.

- **Log off Disconnected sessions after:** From the drop-down list, select the time to sign out disconnected users.

Note: By default, users can disconnect from an AVD session without signing out and ending the session. When a session is in a disconnected state, running programs are kept active even though the user is no longer actively connected. By default, these disconnected sessions are maintained for an unlimited time on the server.

If you enable this policy setting, disconnected sessions are deleted from the server after the specified amount of time. To enforce the default behavior that disconnected sessions are maintained for an unlimited time, select **Never**. If you have a console session, disconnected session time limits do not apply.

- **Disconnect Idle Session After::** From the drop-down list, select the maximum amount of time that an active session can be idle (without user input) before it is automatically disconnected.

Note: If you enable this policy setting, the idle session is disconnected after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply.

- **Disconnect Active session after:** From the drop-down list, select the maximum amount of time that a session can be active before it is automatically disconnected. The recommended setting: **Not configured**.

Note: If you enable this policy setting, active sessions are automatically disconnected after the specified amount of time. The user receives a warning two minutes before the session disconnects, which allows the user to save open files and close programs. If you have a console session, active session time limits do not apply.

- **Log off Empty RemoteApp sessions after:** From the drop-down list, select the amount of time a user's RemoteApp session remains in a disconnected state after closing all RemoteApp programs before the session is signed out.

Note: By default, if a user closes a RemoteApp program, the session is disconnected but it is not signed out. If you enable this policy setting, when a user closes the last running RemoteApp program associated with a session, the RemoteApp session remains in a disconnected state until the time limit that you specify is reached. When the time limit specified is reached, the RemoteApp session is signed out. If the user starts a RemoteApp program before the time limit is reached, the user reconnects to the disconnected session on the AVD session host VM.

If you disable or do not configure this policy setting, when a user closes the last RemoteApp program, the session is disconnected but it is not signed out.

- **Log off, instead of disconnecting, idle and active sessions:** From the drop-down list, select the option to specify whether to end an active or idle session that has timed out instead of disconnecting it.

Note: You can use this setting to sign out a session after time limits for active or idle sessions are reached. By default, sessions are disconnected (not signed out) when they reach their time limits.

If you disable this policy setting, idle and active sessions that reach their time limit are disconnected even if specified otherwise by the server administrator.

This policy setting only applies to time-out limits that are explicitly set by the administrator. This policy setting does not apply to time-out events that occur due to connectivity or network conditions.

- **Apply to existing hosts:** Select this option to apply the modified session time limits to existing hosts.

- **Restart VMs:** Select this option to restart session host VMs after updating session timeouts.
- **Process Host in Groups Of:** Type the number of concurrent operations when applying the change.
- **Number of failures before aborting:** Type the number of failed tasks before the process stops.
- **Schedule:** Toggle on the Schedule to apply the changes at a selected time.
 - **Start Date:** Type the date to start.
 - **Time Zone:** From the drop-down list, select the time zone for the Start time.
 - **Start Time:** From the drop-down lists, select the time to start.
 - **Repeat:** From the drop-down list, select the recurring schedule, if desired.

Note: The drop-down has the option **After Patch Tuesday**. This allows you to create a recurring schedule based on [Patch Tuesday](#).

- **Days After:** If you selected **After Patch Tuesday**, type the number of days after Patch Tuesday to run the scheduled task.

4. Once you have entered all the desired information, select **Save** or **Save & close**.

Publish Remote Applications to Users

You can use Nerdio Manager to easily publish applications (RemoteApps) within Azure Virtual Desktop. These applications may be restricted by Application Group, if required, allowing administrators to publish different apps to different users from the same host pool.

Add App Groups to Host Pools

Application Groups allow the assignment of users and groups to desktops and RemoteApps. This helps simplify application management because applications can be managed by app groups instead of individual users.

Note: There must be at least one app group associated with a host pool.

To add an app group to a host pool:

1. Select the host pool you want to work with.
2. From the action menu, select **Manage > App groups**.
3. Enter the following information:
 - **RemoteApp app groups:** Type the name(s) of the app groups for RemoteApps.

Note: A host pool may have multiple RemoteApp app groups.

- **Desktop app group:** Type the name of the Desktop app group.

Note: A host pool may only have one Desktop app group.

4. Once you have entered the desired information, select **OK**.

Publish RemoteApps to Users

RemoteApps gives the user the ability to launch a single application without having to launch the full desktop experience. For example, the user can launch Excel without having to sign in to a desktop. This saves on session host resources because the users do not have to use a full desktop. So, in our Excel example, you might be able to have 10 users working with Excel as a RemoteApp, but had the users connected as a full desktop, the session host might have been able to handle fewer users. That means you would have to deploy additional session hosts to handle all the Excel users.

To publish a remote application to users:

1. Select the host pool with RemoteApp (Pooled) you want to work with.
2. From the action menu, select **Applications > RemoteApps**.

3. Select **Add RemoteApp**.

Notes:

- When adding the RemoteApp, the host must be switched on and the applications that you want to publish must be already installed.
- If the host pool has multiple RemoteApp app groups, a specific RemoteApp app group must be selected. By publishing different applications to different Application Groups, administrators can control access to these applications via group membership. This allows user groups to be served different applications from the same host pool.

4. Enter the following information:

- **Application Source:** From the drop-down list, select application's source.

Note: You may select one of the following application source types:

- **Installed on host:** The apps are installed locally on the session host VM.
- **App Attach Package:** An MSIX App Attach package.
- **File Path:** You may select a specific file path to the target application. This can help in scenarios where the target application does not register itself with the Windows installer, or where portable applications are required.

- **Application:** From the drop-down list, select the application.
- **Name:** Type the name of the RemoteApp.

Note: The **Name** is visible to the user unless overridden by the **Friendly Name**.

- **Friendly Name:** Optionally, type the friendly name that is visible to the user.
- **Description:** Type the description that is visible to the admin.

- **File Path:** Type the path to the application executable on the session host.
- **Icon Path:** Optionally, type the path to an icon file to be used for this RemoteApp when it appears in the user's Remote Desktop feed.
- **Icon Index:** Optionally, type the numeric icon index in the icon file.

For Installed on Host:

- **Command Line Setting:** Select this option to require a command line setting.

Note: This option should be selected if a command line value is required.

- **Command Line:** Type the command line to pass to the executable when launching the RemoteApp.

5. Once you have entered the desired information, select **OK**.

The authorized host pool users now need to be assigned to the RemoteApp Group that contains the newly published RemoteApp.

Note:

- Host pool users are not automatically assigned to that host pool's RemoteApp Groups. Each user must be individually assigned to the appropriate RemoteApp Group.
- From the action menu, you can **Edit** or **Delete** published apps.

Related Topics

Remote Applications Maintenance Mode

Accelerated Networking on Session Host VMs

The Azure VM accelerated networking feature is available in some of the larger Azure VMs.

This feature is useful for enterprise organizations and IT professionals who need to deploy, manage, and optimize large amounts of Azure Virtual Desktops. It speeds up networking performance of individual VMs.

To enable and apply accelerated networking on session host VMs in the workspace:

1. Locate the host pool you want to work with.
2. From the action menu, select **Properties > VM Deployment**.
3. Select **Enable Accelerated Networking for VMs that support it**.

Note: If this feature is not supported on your Azure VM, it is not enabled. See this Microsoft [document](#) for more information.

4. Select **Save** or **Save & close**.

The process is automatically performed.

Security

This section discusses topics related to permissions and access needed to install and work with Nerdio Manager.



Nerdio Manager is Veracode verified

Azure Permissions and Nerdio Manager

Nerdio Manager is an Azure application that is deployed from the Azure Marketplace and runs inside your own Entra ID tenant and Azure subscription. It requires certain permissions during installation, configuration, and ongoing use.

Tip: See the following document for a deep dive into the Azure permissions and Nerdio Manager: [Nerdio Manager for Enterprise - Permissions](#).

Installation Permissions

The Entra ID user performing the installation of Nerdio Manager requires the following permissions:

- **Global Administrator** role in Entra ID.
- **Owner** role in the Azure subscription.

Note: These elevated permissions are needed only for the initial installation and configuration process, and are not necessary for the ongoing use of Nerdio Manager.

When Nerdio Manager is installed, it has the following API application permissions in Azure:

Service	Permission	Function
Azure Resource Manager	Subscription Reader Subscription Backup Reader	List the available resources in the Azure subscription and make requests on behalf of the user.
Microsoft Graph	Application.Read.All (delegated) AppRoleAssignment.ReadWrite.All (delegated) Application.ReadWrite.All (delegated)	Manage the Nerdio Manager application service principal and assign the users to the Nerdio Manager application to enable user sign in.
Microsoft Graph	Organization.Read.All (delegated) Organization.Read.All (application)	Read organization-level information, such as tenant name.
Microsoft Graph	User.Read (delegated) User.ReadBasic.All (delegated) User.Read.All (application) User.Read.All (delegated) Group.Read.All (application) Group.Read.All (delegated) GroupMember.Read.All (delegated)	Read the Entra ID groups and membership for app group assignments.
Microsoft Graph	Offline_access (delegated) Openid (delegated) profile (delegated)	Allow user sign in and delegated actions.

Service	Permission	Function
	(Optional) Mail.Send (delegated)	
Azure Service Management	user_impersonation (delegated)	Make requests to Azure on behalf of the user.
Windows Virtual Desktop	TenantCreator (application)	(AVD Classic/V1) Create the AVD tenants.
Windows Virtual Desktop	user_impersonation (delegated)	(AVD Classic/V1) Make requests on behalf of the user.

Note: `Group.Read.All` and `User.Read.All` application-level API permissions can be removed in version 4.0 and later. Removing these permissions has the following implications:

- REST API cannot be used to assign users to host pools without `User.Read.All` application-level permission.
- If using Installed Apps management with existing rulesets, after removing `Group.Read.All` application-level permissions, be sure to open each ruleset and save it.

Subscription Permissions

While activating Nerdio Manager licensing subscription, a new SaaS subscription object Azure resource is created on the Azure subscription, which allows Nerdio Manager to charge for license consumption as a 3rd party service on the Azure bill. In order to configure a SaaS subscription object, because it causes additional costs to be included on the subscription, the user completing the configuration must be a **subscription owner**.

A new Entra ID application registration specific for Nerdio Manager's billing is also created automatically as part of the resource deployment. This application is granted the below

permissions in order to authenticate as your user on behalf of your Azure tenant, and register the SaaS subscription object as being tied to your Azure subscription. These permissions allow the billing application to inform Nerdio Manager's licensing service the following details:

- Who is completing the purchase.
- Which SaaS subscription object is used for billing.
- Which Entra ID tenant you are connecting from.

Note: These are the same permissions being granted to the billing application as are granted to the primary Nerdio Manager application above.

Service	Permission	Function
Microsoft Graph	openid, profile, User.Read (delegated)	Allows user sign in (name & Azure tenant ID are shared).

Configuration Permissions

Once the Nerdio Manager application is installed, there are several configuration actions that can be taken inside of Nerdio Manager to "link" it to existing Azure resources or create new ones. These actions require the requesting user (that is, the user signed in and performing the action via Nerdio Manager) to have certain permissions on the Azure resources that are being used.

Action	Permissions Required
Link a resource group	The requesting user must be an Owner on the resource group being linked.
Link a network	The requesting user must be an Owner on the vNet that is being linked (or the resource group that contains the vNet).
Link an additional Azure subscription	The requesting user must be an Owner on the subscription that is being linked.

Action	Permissions Required
Switch the AVD object model from Classic to ARM	The requesting user must be a Global Administrator in the Entra ID in order to grant the required admin consent.
Enable Sepago Azure monitoring	The requesting user must be an Owner on the selected resource group for deployment of the Log Analytics resources and permission assignment.
Create Azure Files shares	The requesting user must be a Contributor on the selected resource group for the storage account deployment. To join a newly created Azure Files share to Active Directory, the selected AD profile must have permissions to create ServicePrincipalName objects (See Permissions Required to Join Azure Files Share to Domain (Active Directory) for additional details.)
Create Azure NetApp Files volumes	The requesting user must be a Contributor on the selected resource group for NetApp account deployment and the vNet containing the NetApp Files subnet.
Create AVD ARM host pools	The requesting user must be a Contributor on the resource group in which the host pool is being created. To allow Nerdio Manager to manage app group membership, the requesting user must be an Owner on the resource group into which the host pool and app group are being deployed.

Action	Permissions Required
Add access to the Nerdio Manager for other users	The requesting user must be an AVD Admin in Nerdio Manager.
Associate session host VMs from previous AVD deployment	The requesting user must be a Contributor in the resource group that contains the VMs.

Ongoing Use Permissions

When the Nerdio Manager application is installed and configured, no user permissions in Azure are required to manage the configured AVD environment via Nerdio Manager. Most actions in Nerdio Manager run on Nerdio Manager on behalf of the signed in user.

Note: There are several RBAC roles available. See [Role-based Access Control \(RBAC\) in NME](#) for details.

Role-based Access Control (RBAC) in Nerdio Manager

You can use Role-based Access Controls (RBAC) to allow users in your organization to sign in to Nerdio Manager and control which actions they can perform once signed in.

The following roles are available:

- **AVD Admin:** A user with the AVD Admin role has complete access to all areas of Nerdio Manager. Only AVD Admins can manage users and roles.
- **Desktop Admin:** A user with the Desktop Admin role has complete access to user sessions, the ability to view Host Pools, power on/off/restart session hosts, but does not have the ability to add/remove hosts or change any host pool settings. This role also allows for full access to Desktop Images and Scripted Actions.
- **Help Desk:** A user with the Help Desk role has access to manage user sessions only.
- **Reviewer:** A user with the Reviewer role has view-only access to all areas of Nerdio Manager. They cannot make edits and save changes.

- **End User:** A user with the End User role can view and manage their own sessions (message, sign out, disconnect). Personal desktop users can restart, power off, and power on their personal desktops.

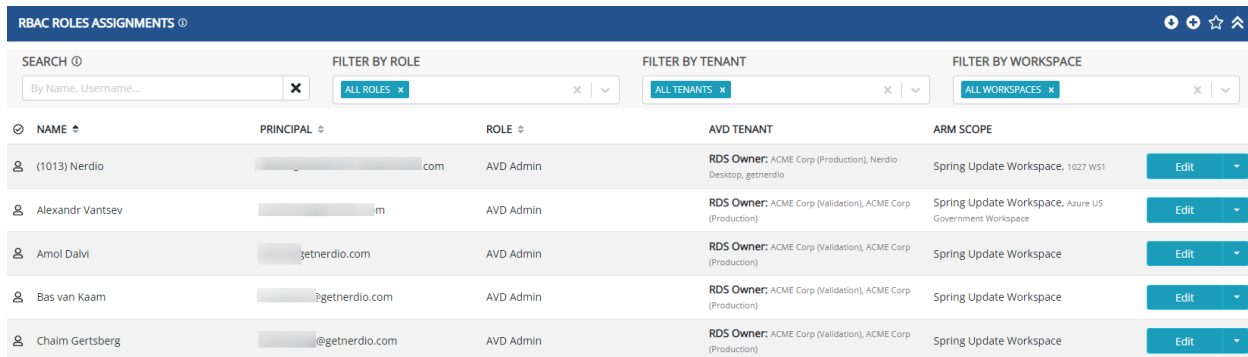
For more information about custom roles, see "Role-based Access Control (RBAC): Custom Roles" on page 310.

Companion Video

Select this [link](#) for a deep dive into RBAC.

Users and Roles Management

- Navigate to **RBAC Roles > Assignments**. The list of users is displayed.



NAME	PRINCIPAL	ROLE	AVD TENANT	ARM SCOPE	
(1013) Nerdio	...com	AVD Admin	RDS Owner: ACME Corp (Production), Nerdio Desktop, getnerdio	Spring Update Workspace, 1027 W51	Edit
Alexandr Vantsev	...m	AVD Admin	RDS Owner: ACME Corp (Validation), ACME Corp (Production)	Spring Update Workspace, Azure US Government Workspace	Edit
Amol Dalvi	...getnerdio.com	AVD Admin	RDS Owner: ACME Corp (Validation), ACME Corp (Production)	Spring Update Workspace	Edit
Bas van Kaam	...getnerdio.com	AVD Admin	RDS Owner: ACME Corp (Validation), ACME Corp (Production)	Spring Update Workspace	Edit
Chaim Gertsberg	...@getnerdio.com	AVD Admin	RDS Owner: ACME Corp (Validation), ACME Corp (Production)	Spring Update Workspace	Edit

Notes:

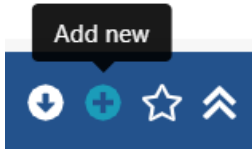
- The search section at the top allows you to search by various fields, including name, username, role, and Workspace.
- You can have the system list up to 1,000 rows on a single page. This is particularly useful when you are looking at a list of end users, which can often be hundreds or thousands.
- Select the down arrow next to **Edit** to display an action menu.

Add Users to Roles/Workspaces

You can add users to Roles/Workspaces.

To add users to Roles/Workspaces:

1. Navigate to **RBAC Roles > Assignments**.
2. In the upper right side, select the **Add new** icon or select the **Add** button.



3. Enter the following information:
 - **Role:** From the drop-down list, select a role.
 - **Users/Groups:** From the drop-down list, select the users/groups you wish to grant access to.
 - **AVD Tenant:** From the drop-down list, select the AVD tenant(s) you wish to grant access to.
 - **Workspace:** For Workspaces roles, from the drop-down list, select the Workspace(s) the user should have access to.
 - **Images:** For Desktop Images roles, from the drop-down list, select the Desktop Image(s) the user should have access to.
 - **Host Pools:** For Host Pool roles, from the drop-down list, select the Host Pools(s) the user should have access to.
4. Once you have entered all the desired information, select **OK**.

Notes:

- The changes are logged as a task. You can review the task's status to ensure the task completed successfully.
- Once access has been granted, users may sign in to Nerdio Manager using their Entra ID username and password. Simply share the URL for Nerdio Manager from your browser's address bar with the user. If MFA is being enforced, the user needs to go through the MFA process while signing in.

Edit a User's Roles/Workspaces

You can change a user's role or the Workspaces the user has access to.

To edit a user:

1. Navigate to **RBAC Roles > Assignments**.
2. Locate the user you wish to edit.
3. Select **Edit**.
4. Once you have made the changes, select **OK**.

Note: The changes are logged as a task. You can review the task's status to ensure the task completed successfully.

Remove User Access

You can prevent a user from accessing Nerdio Manager by removing the user's access.

To remove a user's access:

1. Navigate to **RBAC Roles > Assignments**.
2. Locate the user you wish to work with.
3. From the action menu, select **Remove access**.
4. On the confirmation window, select **OK**.

Note: The changes are logged as a task. You can review the task's status to ensure the task completed successfully.

Role-based Access Control (RBAC): Custom Roles

You can create custom roles to control access to all areas of Nerdio Manager. Custom roles define the scope and level of access and can be assigned to users and security groups. Users

can access modules in read-only or full-access mode.

To create a custom role:

1. Navigate to **RBAC Roles > Definitions** .
2. Select **Add**.
3. Enter the following information:
 - **Name:** Type the custom role's name.
 - **Description:** Type a description of the custom role.
 - **Modules:** Select all the applicable modules and modes.

Module	Modes
Dashboard	<ul style="list-style-type: none"> • Read Only
Workspaces	<ul style="list-style-type: none"> • Read Only • Full Access • Manage hosts: Allow users to manage hosts within assigned host pools. • Manage assignments: Allow users to manage assignments within assigned host pools. • Manage sessions: Allow users to manage sessions within assigned host pools. • Manage power state: Allow users to manage the power state of the sessions within assigned host pools. • Manage drain mode: Allow users to manage the drain mode of the sessions within assigned host pools.

Module	Modes
	<ul style="list-style-type: none"> • Run scripted actions: Allow users to run scripted actions within assigned host pools.
Desktop Images	<ul style="list-style-type: none"> • Read Only • Full Access
Intune	<p>Global Roles:</p> <ul style="list-style-type: none"> • Read Only • Full Access <p>Read Only Roles:</p> <ul style="list-style-type: none"> • Read Devices • Read Policies • Read Applications and App Policies • Read Update Rings and Policies • Read Scripts • Read BitLocker • Read Antivirus • Read User Experience • Read User Groups • Read Device Location <p>Manage Roles:</p> <ul style="list-style-type: none"> • Manage Devices • Manage Devices Privileged • Manage BitLocker

Module	Modes
	<ul style="list-style-type: none"> • Manage Antivirus • Manage Device Groups • Manage User Groups • Manage Locate Device • Manage Policies • Manage Applications and App Policies • Manage Update Rings and Policies
Intune > Windows 365	<ul style="list-style-type: none"> • Read Only • Full Access
App Attach	<ul style="list-style-type: none"> • Read Only • Full Access
UAM > Deployment Policies	<ul style="list-style-type: none"> • Read Only • Full Access
UAM > App Groups	<ul style="list-style-type: none"> • Read Only • Full Access
UAM > Catalog	<ul style="list-style-type: none"> • Read Catalog • Manage Catalog: Allow users to manage UAM catalogs and performs tasks such as importing and deploying apps. • Manage Shell App Parameters: Allow users to manage Shell App parameters.
Scripted Actions	<ul style="list-style-type: none"> • Read Only • Full Access

Module	Modes
Monitoring	<ul style="list-style-type: none"> • Read Only
Storage > Azure Files	<ul style="list-style-type: none"> • Read Only • Full Access • Manage Profiles: Allow users to manage FSLogix profiles without the need for an active user session and without the need to provide full control to the file share.
Advisor > Modeler	<ul style="list-style-type: none"> • Read Only • Full Access
Advisor > Recommendations	<ul style="list-style-type: none"> • Read Only • Full Access
Advisor > Rules	<ul style="list-style-type: none"> • Read Only • Full Access
Storage > Azure NetApp Files	<ul style="list-style-type: none"> • Read Only • Full Access
Storage > Log Analytics	<ul style="list-style-type: none"> • Read Only • Full Access
Desktops	<ul style="list-style-type: none"> • Full Access

4. Once you have entered all the desired information, select **OK**.

Note: From the list of definitions, you can edit or delete a custom role.

For more information, see [Role-based Access Control \(RBAC\) in Nerdio Manager](#).

Manage user sessions

You can use Nerdio Manager to manage active and disconnected user sessions within the selected workspace.

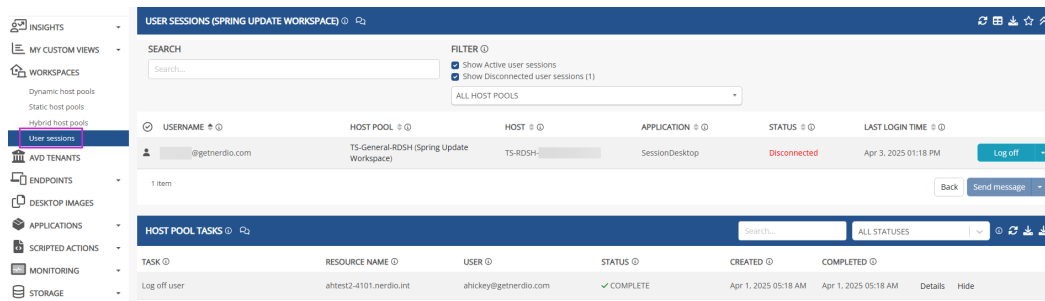
- RBAC permissions are required to manage user sessions. See "Role-based Access Control (RBAC) in Nerdio Manager" on page 307 for details. In addition, the user needs permission for RDP.
- The host pool must be enabled to allow selected non-admin users or groups to shadow sessions. See "Host pool VM deployment" on page 280 for details. In addition, you also need network connectivity to the desktop.

Note: You can also select multiple user sessions and perform actions on those user sessions in bulk.

When using new UI, see "New UI: Manage user sessions" on page 317.

To manage user sessions:

1. Navigate to **Workspaces**.
2. From the list of workspace(s) displayed, select the desired workspace.
3. Select **User sessions**.
4. The **User sessions** window opens. It displays all the active or disconnected user sessions across the host pools in this workspace.




5. Use the **Search** feature to search for:

- Username.
- Host name.

6. Use the **Filter** feature to filter by:

- Show active user sessions.
- Show disconnected user sessions.
- Selected host pool.

7. To download user session information as a CSV file, select the  icon from the user sessions bar at the top.

8. You can select and perform these actions with the users:

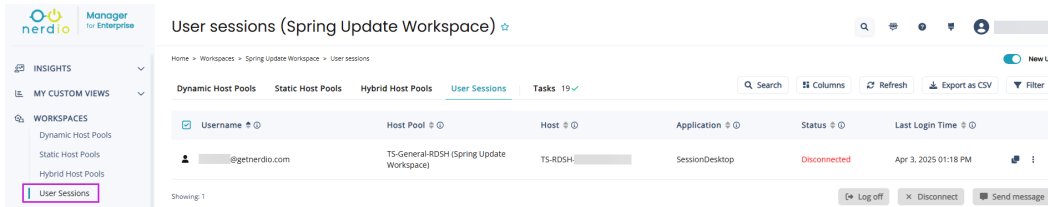
- **Send message:** Send a message to the user session.
- **Disconnect:** Disconnect the user session.
- **Log off:** Sign out the user session.
- **Shadow session:** Shadow (remote access) the session and provide on-screen support.
- **Log off and flush:** Log off and archive or delete user profiles in order to troubleshoot user issues.

New UI: Manage user sessions


When using classic UI, see "Manage user sessions" on page 315.

To manage user sessions:

1. Navigate to **Workspaces**.
2. From the list of workspace(s) displayed, select the desired workspace.
3. Select **User sessions**.
4. The **User sessions** window opens. It displays all the active or disconnected user sessions across the host pools in this workspace.



5. Select **Search** to open the search feature to search for:
 - Username.
 - Host name.
6. Select **Columns** to enable column visibility for application and last login time information.
7. Select **Refresh** to update the information displayed.
8. Select **Export as CSV** to download a CSV file containing user session information.
9. Use the **Filter** feature to filter by:
 - Show active user sessions.
 - Show disconnected user sessions.
 - Selected host pool.

10. You can select and perform these actions with the users by selecting the corresponding button or the more options  menu:
- **Send message:** Send a message to the user session.
 - **Disconnect:** Disconnect the user session.
 - **Log off:** Sign out the user session.
 - **Shadow session:** Shadow (remote access) the session and provide on-screen support.
 - **Log off and flush:** Log off and archive or delete user profiles in order to troubleshoot user issues.

Reset FSLogix user profile

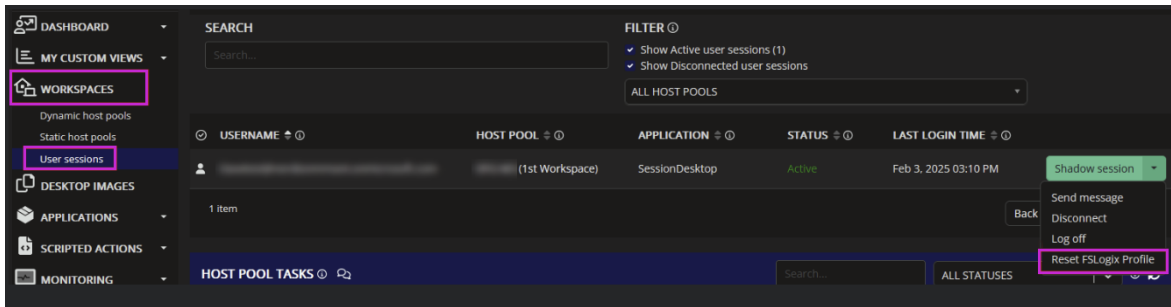
Consider resetting the FSLogix user profile to resolve or troubleshoot any profile-related issues.

Note:

- Resetting the FSLogix profile signs the user out and deletes their profile.
- You need admin permissions to reset the FSLogix user profile.

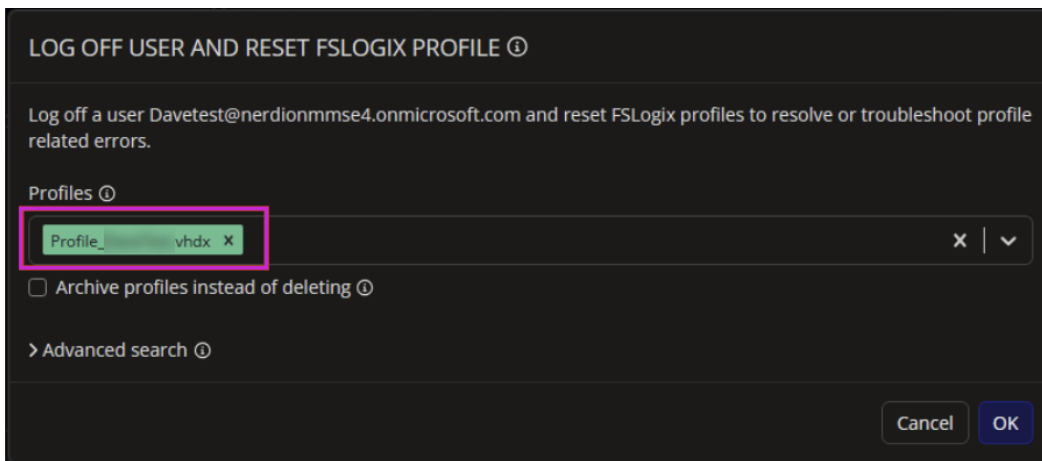
To reset an FSLogix user profile:

1. Navigate to **Workspaces** and select the desired workspace.
2. Go to **User sessions** and locate the user whose profile you wish to reset.
3. From the **Shadow session** action menu, select **Reset FSLogix Profile**.



The **Log off user and reset FSLogix profile** dialog box opens.

4. Under **Profiles**, from the drop-down list, select the profile that you wish to reset.
5. Select **OK**.



Windows 365

This section discusses topics related to Windows 365.

Windows 365: Enable and configure Cloud PCs

The following topics discuss how to enable and configure Windows 365 Cloud PCs.

Enable Windows 365 in Nerdio Manager

The following procedure allows you to enable the Windows 365 environment in Nerdio Manager.

Important:

- The user who enables Windows 365 must be a **Global Administrator** in order for the process to complete successfully.
- An **Intune license** must be present in the Entra ID tenant where Nerdio Manager is installed.
- A **Windows 365 license** must be present in the Entra ID tenant where Nerdio Manager is installed.
- **Entra ID** also requires approval on an application permission request consent page. If a 'grant consent on behalf of my organization' selection is available, be sure to approve.

To enable Windows 365 in Nerdio Manager:

1. Navigate to **Settings > Integrations**.
2. In the **Intune** tile, next to **Current status**, select **Disabled** to enable Intune.
3. Enter the following information:
 - **Current Status:** Toggle this option **On** to enable Intune. Toggle this option **Off** to disable Intune.

- **Configurable Features:** Select all the desired configurable features and their related permissions.

Note: See Unified Endpoint Management: Intune Integration - Granular Permissions for a deep dive into the features and permissions.

- **Device Visibility Scope Limitations:** In this section, select the desired device visibility scope limitations.
 - **Device type scope:** Optionally, from the drop-down list, select the device type (s) to manage.

Note: By default, all Intune devices are included. Optionally, device management can be limited to AVD hosts, Windows 365 Cloud PC, and/or physical devices.

- **Limit by Entra ID group:** Optionally, from the drop-down list, select one or more Entra ID groups to restrict management to include only devices for the users defined within the selected groups.

Note: This option works in combination with the selected **Device type scope**.

- **Include devices that have no primary user:** Select this option to include any devices that have not been assigned to a user.

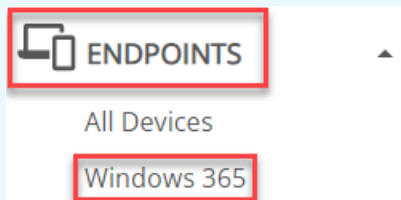
Note: This option is limited by the selected **Device type scope**, but ignores any selected **Limit by Entra ID group** rules.

4. Once you have entered all the desired information, select **Save**.

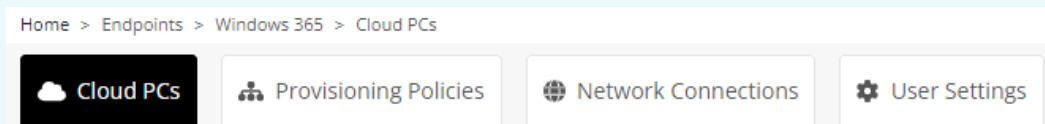
Windows 365 is enabled in your install of Nerdio Manager.

Notes:

- Nerdio Manager now walks you through the process of creating a provisioning policy. You may cancel this and create a provisioning policy later. See "Create a provisioning policy" on page 326 for more information.
- A new **Endpoints > Windows 365** option on the main menu is now available. See "Hide or display individual Cloud PC hosts page" below for more information.



- At the top of the window, use the tabs to navigate to the desired Windows 365 feature.

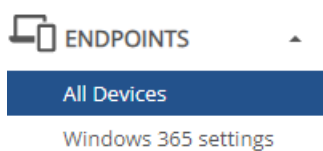


Hide or display individual Cloud PC hosts page

Nerdio Manager allows you to hide or display the individual Cloud PC hosts page.

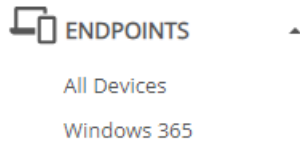
Note: All the functionality (restart, resize, etc.) is available no matter whether you hide or display the individual hosts page.

When you hide the individual Cloud PC hosts page:



- The Cloud PCs hosts are shown in **Endpoints > All Devices**, which can be filtered for Windows 365 Cloud PCs only.
- **Endpoints > Windows 365 settings** only contains settings and no hosts.

When you display the individual Cloud PC hosts page:



- The Cloud PCs hosts are shown in **Endpoints > Windows 365 > Cloud PCs** tab.
- **Endpoints > Windows 365** also contains the settings.
- The Cloud PCs hosts are also shown in **Endpoints > All Devices**.

To hide or display the individual Cloud PCs hosts page:

1. Navigate to **Settings > Azure Environment**.
2. In the **Intune (Unified Endpoint Management)** tile, select **Enabled**.

CONFIGURE INTUNE

Intune integration can be limited by device type or Entra ID user group.

CURRENT STATUS ⓘ

CONFIGURABLE FEATURES

<input checked="" type="checkbox"/> Intune managed devices* ⓘ	<input type="radio"/> Read-only	<input checked="" type="radio"/> Manage
<input checked="" type="checkbox"/> Group membership ⓘ	<input type="radio"/> Read-only	<input checked="" type="radio"/> Manage
<input checked="" type="checkbox"/> Privileged operations ⓘ	<input type="radio"/> Read-only	<input checked="" type="radio"/> Manage
<input checked="" type="checkbox"/> Local Admin Password ⓘ	<input type="radio"/> Read-only	<input checked="" type="radio"/> Manage
<input checked="" type="checkbox"/> Scripts ⓘ	<input checked="" type="radio"/> Read-only	— N/A
<input checked="" type="checkbox"/> Cloud PC ⓘ	— N/A	<input checked="" type="radio"/> Manage

Hide individual Cloud PC hosts page (recommended) ⓘ



3. Under **Cloud PC**, toggle the **Hide individual Cloud PC hosts page** option **On** or **Off** as desired.
4. Select **Save**.

Configure a Windows 365 network connection

Windows 365 Enterprise Cloud PCs require Active Directory with Hybrid Entra ID sync. In order for that to work, you need to configure a network connection.

To configure a Windows 365 network connection:

1. Navigate to **Endpoints > Windows 365 settings** or **Windows 365**.
2. Select the **Network Connections** tab.
3. Select **Add network connection**.
4. Enter the following information:
 - **Name:** Type the name of the network connection.
 - **Network type:** From the drop-down list, select the network type.
 - **Resource Group for cloud PC network cards:** From the drop-down list, select the resource group to contain the network interface cards of the Cloud PC desktops.
 - **Network:** From the drop-down list, select the desired network and sub-net.
5. Once you have entered all the desired information, select **OK**.

Note: The Cloud PC desktops that are created on the selected network are created in the Azure region associated with the network.

- **Active Directory:** From the drop-down list, select the AD profile. This provides the credentials when creating the computer objects as the Cloud PCs come online. AD profiles can be modified under **Settings > Integrations** within Nerdio Manager.

After several minutes, the network connection is created.

Note: After the network connection is created, the Windows 365 service initiates automatic health checks to validate that the provisioning is successful. The health checks may take 30-60 minutes or longer to complete. These must pass before any Cloud PC desktops may be provisioned.

Manage Windows 365 network connections

Nerdio Manager allows you to manage Windows 365 network connections.

To manage Windows 365 network connections:

1. Navigate to **Endpoints > Windows 365 settings** or **Windows 365**.
2. Select the **Network Connections** tab.
3. Locate the network connection you wish to work with.
4. You can perform any of the following functions:
 - Select the **Name** to see the configuration information.
 - Select the **VNet** to open it in Azure.
 - Select the **Domain** to view the domain the network is connected to.
 - Select the **Status** to see the test details.
 - Select **Edit** to change the network connection.
 - From the action menu, select **Health check** to perform a health check on the network connection.
 - From the action menu, select **Delete** to delete the network connection.

Note: Microsoft tests this network on a regular basis to make sure it is still healthy and functioning. If there is a problem with the network, review the test details to find and fix the issue. See this Microsoft [article](#) for more information.

Create a provisioning policy

This feature is only available in the Nerdio Manager **Premium** edition.

A provisioning policy is a combination of a network connection with an image. It then maps the combination to an assignment of security groups in Entra ID. This enables the Cloud PC desktops to be provisioned.

To create a provisioning policy:

1. Navigate to **Endpoints > Windows 365 settings** or **Windows 365**.
2. On the **Policies** tab, select **Add policy**.
3. Enter the following information:
 - **Name:** Type the name of the policy.
 - **Description:** Type the policy's description.
 - **License type:** From the drop-down list, select the license type.
 - **Cloud PC image:** From the drop-down list, select the Cloud PC image. You may select either a Managed Image (created by Nerdio Manager in the **Desktop Images** menu), a Microsoft Gallery Image, or any of the Custom Images uploaded to Endpoint Manager directly.
 - **Language & Region:** From the drop-down list, select the language and region.
 - **Network connection:** From the drop-down list, select the desired network connection. If only one network connection is available, it is selected by default.

Note: From the drop-down list, you can select **Built In Network > Microsoft Hosted Network** to provision Cloud PCs without on-premises AD domain controllers. Both customer-managed and Microsoft-managed VNets are supported. Cloud PCs provision faster and join Entra ID automatically.

4. Once you have entered all the desired information, select **OK**.

The provisioning policy is created.

Edit a provisioning policy

Nerdio Manager allows you to edit an existing provisioning policy.

To edit a provisioning policy:

1. Navigate to **Endpoints > Windows 365 settings** or **Windows 365**.
2. On the **Provisioning Policies** tab, next to the desired provisioning policy, select **Edit**.
3. Enter the following information:
 - **Force apply region change:** Select this option to force apply a change to the provisioning policy's region.

Warning: Cloud PCs are shutdown during this process. Users are disconnected and any unsaved work is lost. Cloud PCs are unavailable for all actions until the region change is complete. The process may take several hours. See [Cloud PC move](#) for details.

- See "Create a provisioning policy" on the previous page for details of the other parameters.
4. Once you have entered all the desired information, select **OK**.

Assign licenses to users

Once you have created the necessary provisioning policies, you can assign users licenses to Cloud PCs.

To assign licenses to users:

1. Open a browser and navigate to your **Microsoft 365 admin portal**. (This is not your Azure admin portal.)

2. Purchase and assign a Cloud PC SKU to a user.

Notes:

- The SKU determines the size of the desktop VM the user receives.
- If the user is a member of a user group that has been assigned to a provisioning policy, and the provisioning policy has a healthy network connection and an assigned image, the desktop automatically comes online in 30-60 minutes.

Access assigned Cloud PCs

Once Cloud PCs are provisioned, the users can access them.

To access your assigned Cloud PC:

1. Open a browser and navigate to windows365.microsoft.com or cloudpc.microsoft.com. Alternatively, use the AVD Remote Desktop Client.
2. Sign in with your Entra ID credentials.
3. In the user self-service portal, all the assigned Cloud PCs are displayed.
4. Select **Open in browser** to open the desired Cloud PC.

Manage Cloud PCs

Nerdio Manager enables you to manage provisioned Cloud PCs.

To manage Cloud PCs:

1. If you hide the individual Cloud PC hosts page, navigate to **Endpoints > All Devices**.
2. If you display the individual Cloud PC hosts page, navigate to **Endpoints > Windows 365**, and select the **Cloud PCs** tab.
3. Use the Cloud PCs list's search and filter capabilities to locate the desired device(s).
4. Locate the device you wish to work with.

- Select the **Device Name** to view the device's details in the Microsoft Endpoint Manager.

Note: Devices with a name of **Not provisioned** indicate the user has a Cloud PC license assigned, but is not included on a provisioning policy.

- Select the **Provisioning Policy** to view the device's policy.
- Select a **Script** to view its run state.
- The **Image** displays what image was used for this device and the SKU.
- Select **Restart** to reboot the device.
- From the action menu, select **Reprovision** to discard the current device and rebuild it.
- From the action menu, select **Resize** to change the user's Cloud PC license to a different SKU.
- From the action menu, select **Restore** to restore the Cloud PC from a restore point.

Windows 365: Use and Configure Desktop Images for Cloud PCs

Note: Before you start this topic, be sure that you have read [Windows 365 Enable and Configure Cloud PCs](#).

This topic contains additional information about using and configuring Windows 365 Cloud PC Desktop Images using Nerdio Manager. Desktop images that you are familiar with in Nerdio Manager can also be used for Cloud PCs.

Warning:

These are the Windows 365 limitations:

- Windows 365 only supports single-session operating systems. That means the multi-session EVD version of Windows 10/11 is not supported.
- Cloud PCs and images only support **Generation 2** VMs in Azure and not Generation 1.
- There is a limit of 20 custom images per Entra ID tenant.

Create a Desktop Image for Cloud PC

Creating a desktop image for Cloud PC is basically the same as creating a regular desktop image, with a few important differences.

To create a new desktop image for Cloud PC:

1. Navigate to **Desktop Images**.
2. Select **Add from Azure library**.
3. Enter the desired Name, Description, etc.
 - In the **Azure Image** drop-down, be sure to select **Windows 10 single-session version**, or **Windows 11 single-session version**, and **Gen 2**.

ADD DESKTOP IMAGE ⓘ

Add desktop image from Azure image library.

NAME:	<input type="text" value="CloudPC-Img"/>	ⓘ
DESCRIPTION:	<input type="text" value="CloudPC Image"/>	ⓘ
NETWORK:	<input type="text" value="Sub3-EastUS-Vnet (hp-Subnet)"/>	ⓘ
	Available IP addresses: 250 (1 of 251 used)	
AZURE IMAGE:	<input type="text" value="Windows 11 (22H2) Enterprise"/> <input type="text" value="Gen2 (single-session)"/>	ⓘ
VM SIZE:	<input type="text" value="D2s_v3 (2C & 8GB)"/>	ⓘ
OS DISK:	<input type="text" value="128 GB (E10 Standard SSD)"/>	ⓘ
RESOURCE GROUP:	<input type="text" value="NME-Resources"/>	ⓘ


- Select **Enable for cloud PCs**.

Note: Selecting this option tells Nerdio Manager to prepare this desktop image for Cloud PC and upload it to the Windows 365 service.


- Enter any other desired desktop image configuration information.
4. Once you have entered all the desired information, select **OK**.

The image comes online, and its Cloud PC status is displayed in the **Cloud PC** column.

Note: This process may take 1-2 hours to complete.

DESKTOP IMAGES TASKS ⓘ			
TASK ⓘ	RESOURCE NAME ⓘ	USER ⓘ	STATUS ⓘ
Upload image to cloud PC	CloudPC-Img	m...io.c om	 IN PROGRESS

5. In the **Cloud PC** column, select **Ready** to open the image in your Intune Admin Center.

NAME ⓘ	VM CONFIG ⓘ	DESCRIPTION ⓘ	LAST UPDATED ⓘ	HOST POOLS ⓘ	CLOUD PC ⓘ
 CloudPC-Img CLOUDPC-IMG 10.50.1.5 (Sub3-EastUS-Vnet/hp-Subnet/eastus)	OS: Windows 11 Enterprise VM Size: D2s_v3 (2C & 8GB) OS Disk: 128 GB (E10/Standard SSD) Resource group: NME-Resources	CloudPC Desktop Image	Jul 3, 2024 10:49 AM		Ready (1.0.0)

Manage Desktop Image for Cloud PC

Nerdio Manager allows to you change a desktop image that was created for Cloud PC.

To change an existing desktop image for Cloud PC:

1. From the main menu, select **Desktop Images**.
2. Locate the desired desktop image make sure it is powered on.

3. From the action menu, select **Generate RDP file**.

GENERATE RDP FILE

Select settings to generate and download RDP file:

- Use local printers when logged in to server
 - Allow copy-paste between local and server
 - Allow audio from server to play locally
 - Allow local microphone to work on server
 - Allow access to local drives from server
-

Cancel

Download

4. Select your RDP options and then select **Download**.
5. Open the RDP file and log in the virtual machine.
6. Make the desired changes on the virtual machine.
7. Back in Nerdio Manager, from the action menu, select **Power off & set as image**.

SET CLOUDPC-IMG AS AN IMAGE ⓘ

Do you want to set CloudPC-Img as an image?

Note: Please ensure that Azure agent is installed and AVD agent is not installed.

Run the following scripted actions before set as image: ⓘ

Off

Applications Management ⓘ

Off

With the schedule set to OFF action will be performed immediately. With schedule turned ON, the task will be performed according to the specified schedule.

SCHEDULE ⓘ

Off

Security type:

Standard

ⓘ

Geographic distribution & Azure compute gallery ⓘ

Off

Save current image as a backup ⓘ

Install App Attach certificates ⓘ

Skip removal of local profiles ⓘ

Enable for cloud PCs ⓘ

Leave desktop image VM running ⓘ

Change log: ⓘ

> Apply tags ⓘ

Cancel

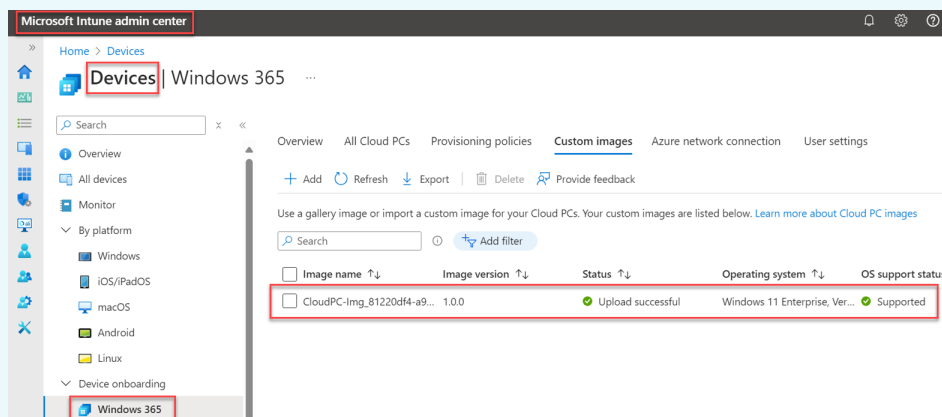
Run now

Note: Since this desktop image was created for Cloud PC, option **Enable for cloud PC** is already selected.

8. Select **Run Now**.

Notes:

- All the changes to the image are stored as an Azure image, as well as uploaded to the Cloud PC service with a new version: [Intune Admin Center](#) > **Devices** > **Windows 365** > **Custom images** tab.



- You can use this new Cloud PC image for Windows 365 provisioning policies.

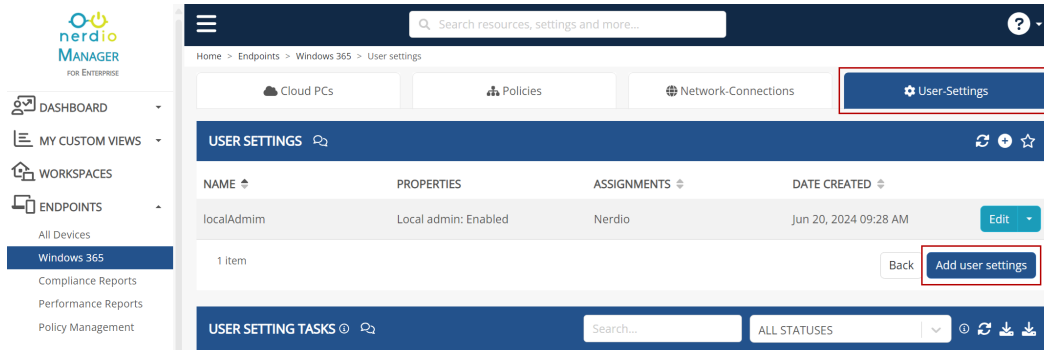
Windows 365: User Settings Policies

This is a new concept in Cloud PC. For more information, please review this [article](#) from Microsoft.

Note: Before you start this topic, be sure that you have read [Windows 365 Enable and Configure Cloud PCs](#).

To add a new user settings policy:

1. Navigate to **Endpoints > Windows 365** or **Windows 365 settings**.
2. Select the **User Settings** tab.



3. Select **Add user settings**.

CREATE USER SETTINGS

Name

Local Admin Enabled ⓘ

Allow user to initiate restore service ⓘ

Frequency of restore-points service ⓘ

 | v

Assignments

 | v

Enable cross region disaster recovery

On

Network connection

 | v | v | v

Cancel

OK

4. Enter the following information:

- **Name:** Type the policy's name.
- **Local Admin Enabled:** Select this option to elevate the end users assigned to this policy to local admins on all their Cloud PCs.
- **Allow user to initiate restore service:** Select this option to give the end user the ability to use snapshots to restore their own Cloud PCs. Otherwise, non-admin users cannot use snapshots to restore the Cloud PC.

- **Frequency of restore-point service:** From the drop-down list, select the time interval to automatically take snapshots (restore points) of a Cloud PC.
 - **Assignments:** Type the name of the group to assign this policy to.
 - **Enable cross region disaster recovery:** Toggle this option **On** to enable cross-region disaster recovery.
 - **Network connection:** From the drop-down list, select the network.
 - **Geography:** From the drop-down list, select the Azure geography.
 - **Region:** From the drop-down list, select the Azure region.
5. Once you have entered all the desired information, select **OK**.

Note: You can edit or delete any of the policies by selecting **Edit** or **Delete** on the User Settings list.

MSIX App Attach

This section discusses topics related to MSIX App Attach.

An MSIX App Attach Image is an expanded container, such as a vhd, vhdx, or cim file, that contains an extracted version of the MSIX packages. An image can contain one or more MSIX packages. The MSIX App Attach images are mounted to the session hosts in the host pool and the applications made available to users who sign in to the session hosts.

Create and Manage MSIX App Attach Images and Host Pool Assignments

This topic discusses how to do the following:

- Upload an MSIX app attach image.
- Upload an MSIX package file.
- Assign an app to a host pool.
- Create a new version of an app.
- Change an app to a new version.

Sample VHD(X) Packages and Certificate

To help you get you started, we created a few VHD(X) packages for some popular applications that you can download and start using in your AVD environment for testing purposes.

Note: These packages are not intended for production purposes. They should be used for proof of concept testing.

Google Chrome

- [VHD](#) file MSIX package
- [MSIX](#) file

Mozilla Firefox

- [VHD](#) file MSIX package
- [MSIX](#) file

Notepad++

- [VHD](#) file MSIX package
- [MSIX](#) file

PuTTY

- [VHD](#) file MSIX package
- [MSIX](#) file

VLC

- [VHD](#) file MSIX package
- [MSIX](#) file

Certificate

- The certificate can be downloaded [here](#).
- The certificate is the same for all the packages.

Upload an MSIX App Attach Image File

Nerdio Manager allows you to upload new versions of packages and automatically apply them to existing host pools. In addition, Nerdio Manager can create an image from an existing MSIX package, or you can upload an image file.

To upload an image:

1. Navigate to **Applications > App Attach**.
2. Select **Upload image**.
3. Enter the following information:
 - **Friendly Name:** Type the name that you want to appear on the images list.
 - **Description:** Type a description.
 - **Storage Location:** From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.

Note: MSIX App Attach does not support Entra Domain Services or Entra ID. This needs to be Active Directory Domain Services (ADDS).

- **Version:** Type the version number of the image that you are uploading. This must be unique.
- **Image File(s):** Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
- **Certificate (.cer) File:** Select the certificate file.

Note: A certificate that was used to create the MSIX package must be installed on all session hosts VMs. If you used a self-signed certificate to create the MSIX package, upload it here and it is automatically installed for you. Alternatively, you can install the certificate on the desktop image and re-image the session host VMs

4. Once you have entered all the desired information, select **Upload**.

The image is uploaded to Nerdio Manager.

Upload an MSIX Package File

This feature is only available in the Nerdio Manager **Premium** edition.

If you do not already have a VHD/VHDX./CIM that contains the image, Nerdio Manager allows you to upload the MSIX file and Nerdio Manager automatically creates a VHD file for you.

To upload an MSIX package file:

1. Navigate to **Applications > App Attach**.
2. Select **Upload MSIX app(s)**.
3. Enter the following information:
 - **Image Name:** Type the image name.
 - **Storage Location:** From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.
 - **MSIX File(s):** Select the MSIX file(s).
 - **Certificate (.cer) File(s):** Optionally, select the certificate file(s).

Note: To expand the MSIX app into a VHDX container, a temporary VM is created to perform the operation and then deleted. It is recommended that you simply let Nerdio Manager handle the temporary VM's configuration. Otherwise, select **Show advanced settings** to specify the temporary VM's details.

4. Once you have entered all the desired information, select **OK**.

The MSIX file is uploaded, and Nerdio Manager begins the process of creating a VM to package the file into a VHDX image.

Assign an App to a Host Pool

Once you have uploaded an MSIX app attach image, you can assign the app to a host pool.

To assign an app to a host pool:

1. Locate the host pool you wish to assign the app to.
2. From the action menu, select **Applications> MSIX App Attach**.
3. When the **Manage MSIX App Attach** window displays, select **Add**.
4. Enter the following information:
 - **Image Source:** From the drop-down list, select the location of the image that contains MSIX packages. The image can be stored in Nerdio Manager's image library or on any SMB file share that session host VMs have access to. If you have uploaded or created MSIX images using Nerdio Manager, select **Image Library**.
 - **MSIX App Attach Image:** From the drop-down list, select an MSIX App Attach image containing the MSIX packages.
 - **Image Version:** From the drop-down list, select the image's version to be added to the host pool.
 - **Packages:** From the drop-down list, select one or more MSIX packages/apps present in the image to make available to users on this host pool.

Notes:

- The package in the file share closest to the host pool's region is prioritized to reduce latency.
- Ensure that the host pool has at least one running session host VM.
- Each VM in the host pool must have certificates that were used to sign MSIX installed. Select **Install certificates** to install them if they aren't already.

5. Once you have entered all the desired information, select **OK**.

The MSIX app is added to the host pool.

Assign an App Attach v2 App to Users and Groups

Once you have uploaded an MSIX App Attach v2, you can assign the app to users and groups.

To assign an App Attach v2 app to users and groups:

1. Navigate to **Applications > App Attach**.
2. Select the **App Attach v2 packages** tab.
3. Locate the App Attach v2 app you want to work with.
4. From the action menu, select **Users and groups**.
5. From the drop-down list, select the **Users and Groups**.
6. Once you have entered all the desired information, select **OK**.

The MSIX app is assigned to the users and groups.

Use the App Attach v2 Package Wizard

The App Attach wizard can be used to deploy App Attach packages to all required AVD host pools automatically, without the need to manually deploy packages.

Note: This feature is applicable to App Attach v2 packages only. Ensure that the required Nerdio App Attach image version is replicated to all required regions before proceeding.

To use the App Attach v2 package wizard:

1. Navigate to **Applications > App Attach**.
2. Select the **App Attach v2 packages** tab.
3. Locate the App Attach v2 app you want to work with.
4. From the action menu, select **Package wizard**.
5. In the **Image** tab, enter the following information:
 - **Image version:** From the drop-down list, select the image version.
 - **Temporary replica:** From the drop-down list, select the version replica used to extract metadata from the selected App Attach image.

- **Temporary host pool:** From the drop-down list, select the temporary host pool used to expand the image.

Note: A temporary host pool is required as a proxy to extract metadata from the selected App Attach image. No changes are made to the pool configuration and any host pool may be used. However, as best practice we recommend the creation of a dedicated App Attach pool. At least one desktop must be running in the pool to proceed.

6. In the **Package** tab, enter the following information:

- **Resource group:** From the drop-down list, select the resource group where the App Attach package is created.

Note: This resource group does not need to be in the same region as the pool assignments, but it is recommended as best practice.

- **Packages:** From the drop-down list, select one or more MSIX packages to make available to users on the selected host pools.

7. In the **Assignments** tab, enter the following information:

- **Host pools:** From the drop-down list, select one or more host pools from the subscription of the selected resource group that are assigned to the package(s).
- **Users and groups:** From the drop-down list, select the authorized users and groups to run the applications included in the selected package(s).

8. In the **Summary** tab, review the selections.

9. Once you have reviewed all the desired selections, select **Run**.

The App Attach wizard task starts. You can see the task's progress in the **App Attach Tasks** window.

Create a New Version of an App

Nerdio Manager allows you to manage multiple versions of an app.

To add a new version of an app:

1. Navigate to **Applications > App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.
3. Locate the image you want to add an app to.
4. From the action menu, select **Upload version**.
5. Enter the following information:
 - **Version:** Type the version number of the image that you are uploading. This must be unique.
 - **Image File(s):** Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
 - **Certificate (.cer) File(s):** Optionally, select the certificate file(s).

Note: A certificate that was used to create the MSIX package must be installed on all session hosts VMs. If you used a self-signed certificate to create the MSIX package, upload it here and it is automatically installed for you. Alternatively, you can install the certificate on the desktop image and re-image the session host VMs.

6. Once you have entered all the desired information, select **Upload**.

The image is uploaded to Nerdio Manager

Change to a New Version of an App

Nerdio Manager allows you to change to a new version an app.

To change to a new version of an app:

1. Navigate **Applications > App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.

3. Locate the image you want to work with.
4. Select **Image versions**. The list of image versions displays.
5. Locate the image version you wish to set as the default.
6. Select **Set as default**. The confirmation window displays.
7. Select **Update host pools where this package is assigned** to assign the new version of the image to the host pools listed above.
8. Select **OK**.

The new version is now the default.

Upload a New Image Version of an App

Nerdio Manager allows you to upload a new image version an app.

To upload a new image version of an app:

1. Navigate **Applications > App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.
3. Locate the image you want to work with.
4. From the action menu, select **Upload a new Image version**.
5. Enter the following information:
 - **Version**: Type the version number of the image that you are uploading. This must be unique.
 - **Storage Location**: From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.
 - **Image File(s)**: Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
 - **Certificate (.cer) File(s)**: Optionally, select the certificate file(s).
6. Once you have entered all the desired information, select **Upload**.

Storage

This section discusses topics related to Azure Files and Azure NetApp Files management.

Azure Files and Azure NetApp Files are a native Azure service often used instead of a traditional IaaS-based virtual machine acting as a file server. It is a more flexible approach offering configurable throughput, including input/output performance characteristics. Azure Files is often used in combination with a user profile management solution such as FSLogix.

Nerdio Manager enables you to work with existing Azure File shares, by linking these to Nerdio Manager. Alternatively, Nerdio Manager can create a completely new Azure Files file share for you, including things such as adding permissions, joining it to the domain, and more.

Nerdio Manager also offers some unique management features not found anywhere else. A great example of this is the ability to auto-scale your Azure Files file share, meaning you are only charged for the storage you consume and you do not have to over provision your file shares leading to higher monthly costs.

Create and manage configured Azure Files shares

The **Azure Files** page contains a list of all the configured and linked Azure Files shares. You can perform various actions on the Azure Files shares such as creating, linking, or managing shares. This includes options such as auto-scale, unlink, setting/changing permissions, closing file handles, and copy the Azure Files UNC path.

Link to an existing Azure Files file share

Nerdio Manager allows you to link to an existing Azure Files share.

To link to an existing Azure Files file share:

1. Navigate to **Storage > Azure Files**.
2. Select **Link Azure Files**.
3. Enter the following information:

- **Storage Account:** From the drop-down list, select the storage account.
 - **File Share:** From the drop-down list, select the file share.
4. Once you have entered all the desired information, select **OK**.

After a few moments, the Azure Files file share is added to Nerdio Manager.

Create a new Azure Files file share and/or storage account

Nerdio Manager allows you to create a new Azure Files file share and/or storage account.

Networking requirements

To ensure proper connectivity to Azure Files shares, make sure the following ports are open.

The additional ports may apply for Azure Government environments.

Port	Protocol	Purpose
53	TCP/UDP	DNS name resolution for Active Directory
88	TCP/UDP	Kerberos authentication (for AD DS integration)
135	TCP RPC	Endpoint Mapper (for AD DS integration)
389	TCP/UDP	LDAP for domain controller communication (for AD DS integration)
443	TCP HTTPS	REST API access, Azure File sync, SMB over QUIC
445	TCP	SMB file access
636	TCP	Secure LDAP (LDAPS)
2049	TCP	NFS protocol access
3268	TCP	Global Catalog (LDAP)
3269	TCP	Secure Global Catalog (LDAPS)

Port	Protocol	Purpose
49152-65535	TCP	RPC Dynamic Ports (for AD DS integration)

To create a new Azure Files file share and/or storage account:

1. Navigate to **Storage > Azure Files**.
2. Select **Add Azure Files**.
3. Enter the following information:
 - **Storage Account:** From the drop-down list, select the storage account.
 - **Storage Account Description:** Type the description of the storage account.
 - **Resource Group:** From the drop-down list, select resource group for the storage account and Azure Files share.
 - **Performance:** From the drop-down list, select performance tier for the share.

Tip: It is strongly recommended that you select **Premium** for the best user experience.

- **Replication:** From the drop-down list, select the type of storage replication.

Note: See [Azure Storage redundancy](#) for more information.

- **File Share Name:** Type the share's name.
- **File Share Description:** Type the share's description.
- **Provisioned Capacity (GiB):** Type the size of the provisioned capacity.
- **Share-level permissions:** Select this option to set default share-level permissions on storage account.

Note:

- **SMB Share Contributor** permission can be used to allow all authenticated users read/write access to the share.
- **SMB Share Reader** can be used to allow all authenticated users read-only access to the share (for example, MSIX app attach).

See [Share-level permissions for all authenticated identities](#) for additional information.

- **Permissions (SMB Share Contributors):** Specify users/groups that have Storage File Data SMB Share Contributor role on the share.

Note: This is required for read/write access to the share.

- **Add users / groups from host pools:** From the drop-down list, select users/groups currently assigned to these host pools to be given Storage File Data SMB Share Contributor role on the share.
- **Join to AD or Entra ID:** Select this option and then from the drop-down list, select an Entra ID or an AD profile to directly join the share.

Note: To use an Azure Files share as a storage location for FSLogix profiles and MSIX App Attach images, the storage account must be integrated with Active Directory, Entra Domain Services, or Entra ID. If you select not to join the storage account to AD or Entra ID, you can do so later. Joining the storage account to AD creates a temporary VM and uses the AD profile credentials to add the storage account as a Computer object in selected AD. Integrating storage account with Entra Domain Services sets the appropriate flag in Azure. Entra Domain Services admin profile credentials are necessary to create a temporary VM to be domain-joined and enable AES-256 encryption. Joining the storage account with Entra ID creates the necessary app registration and provides you with an option to grant needed consents.

- **Create a computer-joined file share:** Select this option to join Azure Files storage accounts to AD by creating either a user object or a computer object in Active Directory.

Note: It is recommended that a user object is used for the domain join process. Please ensure that no policies are in effect that may disable or remove this account or reset its password. If a computer object is selected, ensure this account is excluded from any automated cleanup process. All file shares are created with AES256 encryption enabled.

- **Assign NTFS file-level permissions:** Select this option to have Nerdio Manager assign NTFS file-level permissions to newly created file shares.

Notes:

- This is in addition to assigning Azure RBAC roles selected above.
 - This process automatically creates a temporary VM to perform the permission assignment task.
 - See this Microsoft [article](#) for information about default file permissions used on new Azure Files shares.
-
- **App Attach:** Select this option to grant Authenticated Users Read permission to sub-directories in the share. This is recommended for shares containing App Attach applications.
 - **FSLogix:** Select this option to grant Authenticated Users Modify permission to the root directory in the share, allowing for the creation of FSLogix profile folders. This is recommended for shares containing FSLogix profiles.
-
- **Show advanced settings:** To join Azure Files to the Active Directory, Nerdio Manager creates a temporary VM to perform the operation. Select the settings to be used for this temporary VM.

Tip: It is strongly recommended that you allow Nerdio Manager to use the default settings when creating the temporary VM. That is, we recommend that you do not use the advanced settings.

- **Enable SMB Multichannel:** Select this option to improve the Azure Files Premium performance.
- **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the Azure Files share.

Note: You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

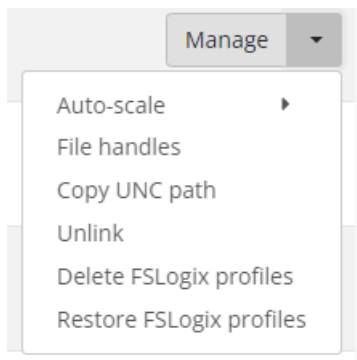
4. Once you have entered all the desired information, select **OK**.

Manage configured Azure Files file shares

Nerdio Manager allows you to manage existing Azure Files file shares.

To manage configured Azure Files file shares:

1. Navigate to **Storage > Azure Files**.
2. Locate the Azure Files share you want to manage.
3. The action menu allows you to perform the following functions:



- **Manage:** Manage the file share's configuration.
 - **Auto-scale:** See "Auto-scale for Azure Files Storage Premium" on page 355 for more information.
 - **Manage Storage Account:** Allows you to enable Entra ID host support. See "Enable support for Entra ID-joined hosts" below for details.
 - **File handles:** Unlock files/Close open file handles.
 - **Copy UNC Path:** Copy the UNC path to the clipboard.
 - **Unlink:** Remove the Azure Files file share from Nerdio Manager.
 - **Delete FSLogix Profiles:** Delete a selected FSLogix profile.
 - **Restore FSLogix Profiles:** Restore a selected FSLogix profile that was previously deleted.
4. From the action menu, select **Manage** to change the Azure Files share's parameters and permissions.

Enable support for Entra ID-joined hosts

Entra ID-joined hosts can now benefit from using App Attach applications, which expands the options for application delivery.

Prerequisites

- You should be familiar with App Attach . See this Microsoft article [App attach and MSIX app attach in Azure Virtual Desktop](#) for details.

Useful information

App Attach supports the following identity providers:

- Microsoft Entra ID
- Active Directory Domain Services (AD DS)

Default file share NTFS permissions:

- BUILTIN\Administrators:(OI)(CI)(F)
- BUILTIN\Users:(RX)
- BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
- NT AUTHORITY\Authenticated Users:(OI)(CI)(M)
- NT AUTHORITY\SYSTEM:(OI)(CI)(F)
- NT AUTHORITY\SYSTEM:(F)
- CREATOR OWNER:(OI)(CI)(IO)(F)

File share NTFS permissions for App Attach:

- BUILTIN\Users:(RX)
- BUILTIN\Users:(OI)(CI)(IO)(GR,GE)
- NT AUTHORITY\Authenticated Users:(OI)(CI)(M)
- CREATOR OWNER:(OI)(CI)(IO)(F)

Area of Usage

Hosts that are going to use App Attach are joined to Microsoft Entra ID

The only mandatory condition for App Attach working on such hosts is that the storage account that stores the App Attach images must be in the same subscription and have **Reader and Data Access** role assignment with **Azure Virtual Desktop** and **Windows Virtual Desktop ARM Provider** members. Storage account can be integrated with any identity provider (Microsoft Entra ID, AD DS) or not integrated at all.

Hosts that are going to use App Attach are joined to AD DS

Mandatory conditions:

- Storage account that stores App Attach images is joined to AD DS
- App Attach NTFS permissions are configured on file share
- Share-level permissions are configured

Variations of share-level permissions configuration:

- **Read-only access for all authenticated identities:** [Default share-level permission](#) with at least **Storage File Data SMB Share Reader** role for all authenticated identities on the storage account.
- **Read-only access for domain computers:**
 1. In Active Directory, create a new Global Security group in an Organization Unit (OU) that is being synched to Entra ID with ADConnect.
 2. Add the Domain Computers to the new group.
 3. Add the newly created security group with at least **Storage File Data SMB Share Reader** role to file share through the Access Control in the Azure Portal.
- Some custom configuration.

Related topics:

- "Create and Manage Configured Azure NetApp Files" on page 360

Auto-scale for Azure Files Storage Premium

A premium file share is billed by provisioned size, regardless of the capacity used. Share sizes can range from 100 GiB to 102,400 GiB. IO and network bandwidth limits scale with the provisioned share size.

When enabled, storage auto-scale grows the provisioned share size in response to anticipated usage demand or increased storage latency. It also decreases the provisioned capacity to reduce costs when the extra performance is no longer needed (not more than once every 24 hours).

Storage auto- scaling with Azure Files can also be used to maintain a specified headroom to avoid running out of space on the volume or capacity pool.

Note: Auto-scale is not available for Azure Files standard storage, because both capacity cost and performance are not controlled by the size of the share.

You must configure these auto-scale parameters:

- Provisioned Size (Quota)
- Scheduled Data Increase (Optional)
- Scaling Logic

To configure and manage auto-scale for Azure Files premium:

1. Navigate to **Storage > Azure Files**.
2. Locate the files share you want to manage.
3. From the action menu, select **Auto-scale > Configure**.
4. Toggle the **Auto-Scale** option to **On**.
5. Enter the **Provisioned Size (Quota)** settings.
 - **Quota unit:** From the drop-down list, select the unit (Relative % or Absolute GiB). Relative is a percentage of currently used capacity.
 - **Minimum size:** Type the minimum size in GiBs or %.

Note: The minimum size is 100 GiB and it may not be smaller than the used capacity. In addition, this defines the minimum buffer that the system always maintains as the user capacity grows. This guarantees the minimum amount of free space in the file share.

- **Maximum size:** Type the maximum size in GiBs or %.
 - **Less than:** Type the size the file share should be increased, below the total file share size, to prevent the uncontrolled system growth..

The **Performance** displays the minimum and maximum configuration values, and displays the performance characteristics.

6. Optionally, toggle **Scheduled Quota Increase On** and enter the settings.

Note: These are the parameters by which you are committed to increase the scheduled quota. The quota is increased during this period and decreased between these periods. This is useful if you have days with peak performance.

- **Days:** From the drop-down list, select the range of days.
- **Hours:** From the drop-down list, select the time zone.
- **Set provisioned size (quota) to:** Type the quota that you commit to increase above the current used capacity.

7. Enter the **Scaling Logic** settings.

Note: Provisioned size (quota) can be decreased only 24 hours after the last quota increase. The quota is increased at the beginning of the period and decreased to the minimum size only at the end of this period.

- **Select auto-scale trigger:** From the drop-down list, select the trigger.

Note: The auto-scale logic configuration allows the scaling engine to determine when to grow or shrink the share. It is based on two available metrics provided by Azure files shares via the API. It describes how long it takes the IOPs to be processed. It can either be the Average Success Server Latency (default) or the Maximum Success Server Latency.

- **Increase the quota (scale out) by:** Type the size the quota is increased according to the Quota unit value specified in the **Provisioned Size (Quota)** section.

Note: When threshold is exceeded, the system continues scaling out until either it reaches the specified Max size, or until the server latency is below the threshold.

- **Decrease the quota (scale in):** Type the size the quota is decreased if the server latency drops below the specified threshold.
8. Once you have entered all the desired information, select **Save** or **Save & close**.

The configured file share appears in the list of shares on the **Azure Files** list.

Related Topics

"Auto-scale for Azure NetApp Files" on page 362

Auto-scale History for Azure Files Shares


The auto-scale history visualization helps you understand auto-scale behavior and how it impacts your deployment.



The following are important auto-scale history features.

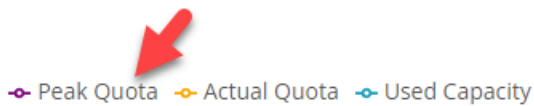
- **Time Range:** At the top of the window, select the desired time range to display.
- **Show:** At the top of the window, select the desired graph(s) to display.
- **Savings:** At the top of the window, you can view auto-scale savings.
- **Zoom In:** For the **Quota (GiB)** graph only, click and drag the mouse over the section of the graph you wish to zoom in on. When you are zoomed in, select **Zoom-out** to restore the full graph.
- **Hover:** You can hover over any part of any graph to see its details. For example:

Dec 15, 2021 12:04 AM

Actual quota: **100 GiB**
 Used Capacity: **57.26 GiB**
 Operation: **Scale-out** up to 110 GiB
 Working hours: **No**
 Reason:
 Success Server Latency (**124.08 ms**) was higher than **20.00 ms** for **5 min**
 Transactions count (**101**) was higher than threshold of 100 for **5 min**

- **Action Points:**
 -  **Scale Out:** This action point indicates that a scale-out event took place. (Red indicates that the scale-out event is costing money.)

-  **Scale In:** This action point indicates that a scale-in event took place. (Green means that the scale-in event is saving money.)
-  **Azure Issue:** This indicates that there was a problem communicating with Azure. If this occurs frequently, please contact Nerdio Manager technical support.
- At the bottom of any graph, select the data set name to toggle on/off the display line associated with that information. For example, select **Peak Quota** to suppress that line on the graph. Select it again to display it.



To view auto-scale history for an Azure Files share:

1. Navigate to **Storage > Azure Files**.
2. Locate the file share you wish to work with.
3. From the action menu, select **Auto-scale > History**.
4. Select the desired time range and the specific graphs to display.
 - **Quota (GiB):** The Quota graph displays the following information about the file share quota:
 - **Peak Quota:** The maximum size of the quota.
 - **Actual Quota:** The actual quota size as it is currently configured.
 - **Used Capacity:** The actual storage used.
 - **Latency (ms):** The Latency graph displays the following information:
 - **Server Latency (avg):** The average time used to process a successful request by Azure Storage. This value does not include the network latency specified in the End-to-End Latency.
 - **End-to-End Latency (avg):** The average end-to-end latency of successful requests made to a storage service or the specified API operation. This value

includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.

- **Transactions:** The Transactions graph displays the number of transactions.
- **Savings%:** The Savings graph displays the savings percentage.

Related Topics

"Auto-scale History for Azure NetApp Shares" on page 366

Create and Manage Configured Azure NetApp Files

This feature is only available in the Nerdio Manager **Premium** edition.

The **Azure NetApp Files** page contains a list of all the configured and linked Azure NetApp files shares. You can perform various actions on the files shares such as creating or managing files shares.

To link to an existing Azure NetApp Files share:

1. Navigate to **Storage > Azure NetApp Files**.
2. Select **Link ANF Volume**.
3. From the drop-down list, select the **NetApp Files Account**.
4. Select **OK**.

After a few moments, the Azure NetApp Files file share is added to Nerdio Manager.

Create an Azure files and/or storage account.

Note: Before proceeding, verify that ANF is available in your Azure region and that your Azure subscription is whitelisted for this service.

1. Navigate to **Storage > Azure NetApp Files**.
2. Select **Add ANF Volume**.
3. Enter the following information:
 - **Active directory:** From the drop-down list, select the active directory.
 - **Resource group:** From the drop-down list, select the resource group.
 - **Network:** From the drop-down list, select the network.
 - **Subnet:** From the drop-down list, select the subnet.
 - **AD-aware DNS Server:** Type the address of the AD-aware DNS server.
4. Once you have entered all the desired information, select **Next**.
5. Enter the following information:
 - **Resource group for ANF account:** From the drop-down list, select a resource group to contain the Azure NetApp Files account objects.
 - **Account name:** Type the ANF account name or leave it blank for it to be automatically generated.
 - **SMB server prefix:** Type the prefix of the computer objects that are to be joined to the AD domain and used for the UNC path. For example: `\\SMB-PREFIX-random\volume\share\folder`.
 - **Volume name:** Type the volume name to be created on the SMB server specified above.

Note: There can be multiple volumes in the same ANF account.

- **Capacity (TiB):** Type the capacity in TiB.

Note: The minimum capacity of an ANF capacity pool is 4 TiB.

- **Performance Tier:** From the drop-down list, select the performance tier of the new capacity pool and volume.

Note: Performance tiers vary in price and throughput (IOPS). See the following Microsoft [document](#) for details.

6. Once you have entered all the desired information, select **Add**.

Related Topics

"Create and manage configured Azure Files shares" on page 347

Auto-scale for Azure NetApp Files

This feature is only available in the Nerdio Manager **Premium** edition.

In Azure storage NetApp files, you have an ANF account that can have multiple capacity pools. Capacity pools are created with a service level (Standard, Premium, Ultra) that determines performance. Within each capacity pool you can have one or more volumes that, in aggregate, cannot exceed the size of this capacity pool. The cost of the ANF storage is determined by the size of the capacity pool, with the minimum size of 4 TiB. You can grow and shrink a capacity pool in increments of 1 TiB, but not smaller than the sum of the volumes that are contained within that capacity pool.

The throughput limit of the ANF storage system is determined by a combination of the quota assigned to the volume and the service level selected.

Storage auto-scaling with ANF is required when you need to dial-up the performance of a particular volume during times of high demand on the storage system, and then dial it back down, on a scheduled basis, when that performance is no longer needed. For example, during sign in/sign out storms from Azure VD machines. Or it could be needed when there is heavy activity on the storage system in the middle of the day and the latency of that volume is detected to be high.

Storage auto- scaling with ANF can also be used to maintain a specified headroom to avoid running out of space on the volume or capacity pool.

To configure and manage auto-scale for Azure NetApp files:

1. Navigate to **Storage > Azure NetApp Files**.
2. Locate the ANF you want to manage.
3. From the action menu, select **Auto-scale > Configure**.
4. Toggle the **Auto-Scale** option to **On**.
5. Enter the **Provisioned Size** settings.

Note: If the volume free space drops below the Min, the system tries to grow the volume. If it cannot grow the volume within the current capacity pool, the capacity pool is always expanded by 1 TiB, and the volume grows at least for 1 TiB.

The volume won't grow beyond the configured maximum size.

- **Mode:** From the drop-down list, select the mode:
 - **Volume only:** Auto-scales the volume without the capacity pool that contains it. The volume is limited to the available free space within the capacity pool, and the capacity pool does not increase automatically.
 - **Volume and capacity pool:** Auto-scales the volume and the capacity pool that contains it (default).
- For **Volume only:**
 - **Size unit:** From the drop-down list, select the unit (Relative % or Absolute GiB). Relative is a percentage of currently used capacity.
 - **Minimum size:** When scaling down, type the minimum size to maintain on the volume. This is evaluated as the currently used capacity + headroom amount.

Note: If the available space drops below the configured minimum free space, the volume is increased to meet the minimum available space. If exceeding capacity pool size, and capacity pool scaling is enabled, then an additional 1 TiB is added to the capacity pool to increase the volume - up to the configured maximum total size.

- **Maximum size:** When scaling out, type the maximum amount the volume should increase. This is evaluated as the currently used capacity + the scaling amount.
 - **Less than:** Define the Max size the volume may grow in order to prevent the uncontrolled system growth. This is limited by the available capacity pool size.
- For **Volume and capacity pool:**
 - **Minimum volume free space:** Type the minimum free to maintain on the volume. If the current free space falls below this threshold, the volume automatically grows along with the capacity pool.
 - **Maximum volume total size:** Type the maximum volume size of the volume in TiBs. The volume and capacity pool combination cannot grow larger than this value.
- **Exceeding the limit should trigger an error:** Select this option to have the auto-scale process trigger an error if the calculated size exceeds the maximum limit.

Note: This allows you to track these errors using notifications. See Configure Email Notifications for details.

The **Size and Performance** calculator displays the minimum and maximum configuration values and displays the performance characteristics.

6. Optionally, toggle **Scheduled-Based Scaling On** and configure the settings.

Note: This is useful if you have peaks in demand on the storage system (for example, when multiple users sign in and sign out during the same time). You can specify more than one period of the peak auto-scaling, after which the system automatically scales down to the Min size. Be sure that the schedules do not overlap.

- **Time Zone:** From the drop-down list, select the time zone.
 - **Days:** From the drop-down list, select the days.
 - **Hours:** From the drop-down list, select the range of hours.
 - **Set provisioned size to:** Type the amount of additional capacity to add to the volume, beyond the current capacity.
7. Optionally, toggle **Latency-Based Scaling On** and configure the settings.
- **Select auto-scale trigger:** From the drop-down list, select the trigger.

Note: This is the average or maximum time used to process a successful request by Azure Storage.

- **Increase volume size (scale out):** The system increases the volume size by the value that you set if the server latency exceeds the specified threshold.
 - **Decrease volume size (scale in):** The system decreases the volume size by the value that you set if the server latency drops below the specified threshold.
8. Once you have entered all the desired information, select **Save** or **Save & close**.

The configured file appears in the list of files on the **Azure NetApp Files** list.

Related topics

- "Auto-scale for Azure Files Storage Premium" on page 355

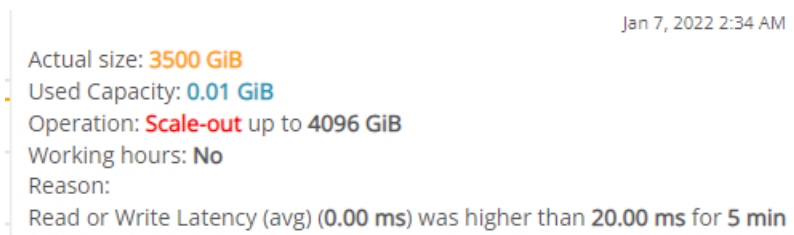
Auto-scale History for Azure NetApp Shares



This feature is only available in the Nerdio Manager **Premium** edition.


The auto-scale history visualization helps you understand auto-scale behavior and how it impacts your deployment.

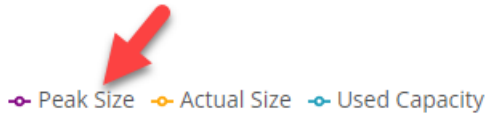
The following are important auto-scale history features.

- **Time Range:** At the top of the window, select the desired time range to display.
- **Show:** At the top of the window, select the desired graph(s) to display.
- **Savings:** At the top of the window, you can view auto-scale savings.
- **Zoom In:** For the **Size (GiB)** graph only, click and drag the mouse over the section of the graph you wish to zoom in on. When you are zoomed in, select **Zoom-out** to restore the full graph.
- **Hover:** You can hover over any part of any graph to see its details. For example:



- **Action Points:**
 -  **Scale Out:** This action point indicates that a scale-out event took place. (Red indicates that the scale-out event is costing money.)
 -  **Scale In:** This action point indicates that a scale-in event took place. (Green means that the scale-in event is saving money.)

-  **Azure Issue:** This indicates that there was a problem communicating with Azure. If this occurs frequently, please contact Nerdio Manager technical support.
- At the bottom of any graph, select the data set name to toggle on/off the display line associated with that information. For example, select **Peak Size** to suppress that line on the graph. Select it again to display it.



To view auto-scale history for an Azure NetApp share:

- Navigate to **Storage > Azure NetApp Files**.
- Locate the file share you wish to work with.
- From the action menu, select **Auto-scale > History**.
- Select the desired time range and the specific graphs to display.
 - Size (GiB):** The Size graph displays the following information about the file share size:
 - Peak Size:** The maximum size of the file share.
 - Actual Size:** The actual size of the file share.
 - Used Capacity:** The current capacity used in the file share.
 - Latency (ms):** The latency graph displays the following information.
 - Read Latency (avg):** The average read latency.
 - Write Latency (avg):** The average write latency.
 - Savings%:** The Savings graph displays the savings percentage.

Related Topics

"Auto-scale History for Azure Files Shares" on page 358

Logs Module

The Logs module allows you to access an audit trail of all tasks performed in Nerdio Manager. In addition, you may configure the logs retention policy.

Access the Logs Module

The Logs module allows you to access an audit trail of all tasks performed in Nerdio Manager.



To access the logs module:

1. Navigate to **Logs**.
2. The following information is displayed:
 - **Task:** The task's name and description.
 - **Resource Name:** The name of the resource the task was performed on.
 - **User:** The user who performed the task.
 - **Status:** The current status of the task.
 - **Created:** The date and time the task was submitted.
 - **Completed:** The date and time the task completed.

Note: The Created and Completed dates are displayed in your local time zone as dictated by your browser.

- **Details:** Select **Details** to view the log entry's details.
3. Optionally, in **Search**, type the Resource name you wish to search for.
 4. Optionally, set the desired filters:

Note: You can start typing the User, Type, or Status to search the respective lists.

- **Filter by Users:** From the drop-down list, select the user(s) you wish to view.
 - **Filter by Types:** From the drop-down list, select the type(s) of activities you wish to view.
 - **Filter by Status:** From the drop-down list, select the job status(es) you wish to view.
 - **Filter by Date:** Select the date range to view.
5. In the upper right side, select the refresh icon  to refresh the list when desired.
 6. In the upper right side, select the export icon  to export the logs in JSON format. The file is downloaded to your browser's default download folder.

Note: Optionally, when prompted, you can include any requested log bundled in the tasks listed below to be included in the export request.

7. Optionally, in the column headings use the **Up-Down arrows** to sort the list.

Configure Logs Retention Policy

You may configure the logs retention policy. That is, you may configure how long to retain the logs, which reduces the database size and the associated costs.

To configure the logs retention policy:

1. Navigate to **Settings > Nerdio environment**.
2. In the **Nerdio Manager database resilience** tile, select the link next to **Log retention period**.
3. Enter the following information:

- **Retention:** From the drop-down list, select the retention period.

Note: Log records older than the specified retention period are automatically deleted.

- 1 year is 365 days.
- 1 month is 30 days.

- **Cleanup Schedule:** If **Retention** is not **Indefinite**, from the drop-down lists select the date and time when the automatic deletion runs.

4. Once you have entered all the desired information, select **OK**.

AI-Powered Personally Identifiable Information Detector

The AI-Powered personally identifiable information (PII) Detector feature automatically scans and identifies PII within Nerdio Manager's logs, ensuring data privacy and regulatory compliance.

See AI-Powered Personally Identifiable Information Detector for full details.

Download Application Insights Exceptions Log

Nerdio Manager runs in an app service, which logs all of its exceptions into an instance of Application Insights. The Application Insights exceptions log can be downloaded to help analyze any errors that may come up in Nerdio Manager or to send to Nerdio technical support for assistance.

To download the Application Insights exceptions log:

1. Navigate to **Settings > Nerdio Environment**.
2. In the **Support** tile, select **Download Applications Insights exceptions**.
3. Type the number of days of logs to download.
4. Select **OK**.

The log is downloaded as a zip file to your browser's default download folder.

Gather Application Insights Logs

While troubleshooting some Nerdio Manager issues, support may request Application Insights logs.

To gather the Application Insights logs:

1. In the Azure portal, search for **Applications Insights**.
2. Select the resource named **nmw-app-insights-xxxxxx**.
3. On the blade on the left side, in the **Monitoring** section, select **Logs**.
4. When presented with the **Getting Started** window, close it.
5. When presented with the **Presets** window, close it.
6. Run the Exceptions query:
 - In the query editor, type **exceptions | where timestamp > ago(10d) | order by timestamp**.
 - Select **Run**.
 - When the query finishes, select **Export > Export to CSV - all columns**.
7. Run Traces query:
 - In the query editor, type **traces | where timestamp > ago(10d) and severityLevel >= 3 | order by timestamp**.
 - Select **Run**.
 - When the query finishes, select **Export > Export to CSV - all columns**.
8. Send the two CSV files as attachments in your reply to the ticket that requested the logs.