



Nerdio Manager for Enterprise Implementation Guide

Table of Contents

Implementation Guide	4
Introduction	4
In this guide:	4
Step #1: Installation	4
In this section:	5
Azure Permissions and Nerdio Manager	5
Nerdio Manager Installation Guide	8
Nerdio Manager Edition Management	18
Activate your subscription	19
Azure Environment: linked networks and resource groups	22
User interface (UI) overview	26
Manage Nerdio Copilot	31
Manage Schedules for Tasks	36
Resource Selection Rules Management	38
Step #2: Desktop Images	43
In this section:	43
Desktop Images	43
Management and lifecycle tasks for imported desktop images	44
Create a Desktop Image	46
Desktop images: set as image	55
Desktop Images Scripted Actions	62
Step #3: Host Pools	64
In this section:	64
Overview of host pools	64
Workspace Management	66
Create dynamic host pools	67
Manage host pool profiles	75
Enable dynamic host pool Auto-scaling	79
Enable personal host pool Auto-scaling	94
Auto-scale: Cost Optimization Session Host VM OS Disk Storage	113
Add a new session host to a dynamic host pool	114
Host Pool AVD Configuration	118
Host pool VM deployment	122
Manage Host Pool User Assignments	131

Configure the Host Pool's Active Directory Settings	131
Start VM on Connect for Pooled Host Pools	133
Configure User Session Time Limits	133
Publish remote applications to users	137
Step #4: Storage	144
In this section:	144
Permissions Required to Join Azure Files Share to Domain (Active Directory)	145
Create and manage configured Azure Files shares	148
Auto-scale for Azure Files Storage Premium	155
Auto-scale History for Azure Files Shares	163
Create and Manage Configured Azure NetApp Files	165
Auto-scale for Azure NetApp Files	167
Auto-scale History for Azure NetApp Shares	171
Step #5: FSLogix and User Profile Management	172
In this section:	173
FSLogix and User Profile Management	173
FSLogix settings and configuration	174
FSLogix per-host pool customization	178
Manage Installed Applications on Host Pools	182
Step #6: MSIX App Attach	189
In this section:	189
Manage App Attach images and packages	189
Manage App Attach Assignments	196
Configure Azure Files Permissions for App Attach	199
Step #7: Role-based Access Control (RBAC)	200
In this section:	200
Role-based access control (RBAC) in Nerdio Manager	201
Role-based access control (RBAC): Custom roles	204
Role-based Access Control (RBAC): Multiple Group Assignments	207

Implementation Guide

Introduction

The *Nerdio Manager for Enterprise Implementation Guide* provides a guided implementation path through the Nerdio Manager for Enterprise documentation — a recommended order of steps for installing, configuring, and getting a new environment ready for users, alongside the Knowledge Base and Setup & Settings sections. It's deliberately narrow: rather than covering every feature Nerdio Manager offers, each step links out to the specific articles you need at that stage.

If you're looking for complete feature-by-feature reference material instead of a step-by-step path, see the **Knowledge Base** and **Setup & Settings** sections.

Questions during implementation? Contact the support team at nme.support@getnerdio.com.

In this guide:

- [Step #1: Installation \(4\)](#)
- [Step #2: Desktop Images \(43\)](#)
- [Step #3: Host Pools \(64\)](#)
- [Step #4: Storage \(144\)](#)
- [Step #5: FSLogix and User Profile Management \(172\)](#)
- [Step #6: MSIX App Attach \(189\)](#)
- [Step #7: Role-based Access Control \(RBAC\) \(200\)](#)

Step #1: Installation

Before you can start managing your Azure environment, you need to install and configure the Nerdio Manager application. This entails granting Nerdio Manager the right Azure permissions, running the installer, activating your subscription, and getting familiar with the management console before you move on to building out your environment.

In this section:

1. [Azure Permissions and Nerdio Manager \(5\)](#)
2. [Nerdio Manager Installation Guide \(8\)](#)
3. [Nerdio Manager Edition Management \(18\)](#)
4. [Activate your subscription \(19\)](#)
5. [Azure Environment: linked networks and resource groups \(22\)](#)
6. [UI Overview \(26\)](#)
7. [Manage Nerdio Manager Copilot \(31\)](#)
8. [Manage Schedules for Tasks \(36\)](#)
9. [Resource Selection Rules Management \(38\)](#)

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:

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).  Note The logged-in user needs owner or user access administrator; Nerdio's service principal then retains contributor on the resource group or VNet.
Link an additional Azure subscription	The requesting user must be an Owner on the subscription that is being linked.
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.
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.

Action	Permissions Required
Create AVD ARM host pools	The requesting user must be a Contributor on the resource group in which the host pool is being created.
Add access to the Nerdio Manager for other users	The requesting user must be an AVD Admin.
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 \(201\)](#) for details.

Nerdio Manager Installation Guide



Note

Before starting, be sure to see Nerdio Manager Installation Preparation Steps.

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, inside a new resource group, or an existing resource group as long as it's empty. Once the installation

is complete, you receive a URL 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.
- Initialize the installation by running an Azure PowerShell script.
- Register your installation with our licensing servers and configure the Nerdio Manager settings.

Companion video

Video: [Install Nerdio Manager](#)

Prerequisites



Note

Before starting the installation process, sign in to your Azure portal as a Global Administrator, or Privileged Role Administrator and Cloud Application Administrator.

- 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 support the deployment of Azure SQL, App Service, Key Vault, Application Insights, and Automation Account in the Azure region you select during the installation 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.
- When using Active Directory or Entra DS, the custom default DNS server setting, specified on the virtual network subnet, must point to either a domain-aware DNS server or an Azure DNS zone.

- When using Windows Active Directory Domain Services (ADDS), ADDS must be synchronized with Entra ID.
- When using Active Directory, you need a user account with permissions 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 those computer objects as needed.
- 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.
 - To ensure best performance, locate the profile storage in the same Azure region as the host pool 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 configuration.
- The Microsoft Desktop Virtualization resource provider must be registered in your Azure subscription.

Install 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.

The **Create NME Plan** page opens.

3. In the **Basics** area, 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. Alternatively, you can select an existing resource group, as long as it's empty.
 - **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 resources are located, and does not determine the location of the AVD session hosts themselves.

- Select **Next**.
4. In the **Resource Names** area, do the following:
 - **Name prefix**: Customize the prefix used for resource names.
 - Select **Next**.
 5. In the **Private Endpoints** area, specify if this install should use private endpoints and restrict Nerdio Manager from being publicly available.

Enter the following information:

- **Enable Private Endpoints**: Enable this option to configure Nerdio Manager to use private endpoints.

 Note

If Nerdio Manager is configured to use private endpoints, the application and its dependencies (SQL Database, Storage Account, Key Vault, App Service, etc.) are no longer reachable through their public internet endpoints. Instead, access is restricted to the customer's virtual network through private IP addresses. You can customize the virtual network and subnet for private endpoints, as well as for the App Service, but this is typically not required.

- **Virtual Network**: From the drop-down list, select the VNet where Nerdio Manager resources will reside.
- **Subnet for Private Endpoints**: From the drop-down list, select the subnet that will host the private endpoints.
- **Subnet for App Service**: From the drop-down list, select the subnet dedicated to the App Service.
- **Restrict App Service public access**: Leave this option unselected.

 Note

If you enable **Restrict App Service public access**, Nerdio Manager will not be available after deployment. Additional manual network configuration will be required.

- Select **Next**.
6. In the **Tags** area, review any custom tags that may be needed, and then select **Next**.

 Tip

You can skip this tab.

7. In the **Review + Create** area, review your selections and select **Create**.

 Note

A confirmation window is displayed, informing you that the deployment is in progress. The deployment usually takes about 10 minutes.

8. When the deployment is complete, select **Go to resource group**.
9. Locate and select the **App Service**.

Initialize

When Nerdio Manager 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 \(Entra ID app registration or Split Identity\) \(13\)](#).

To initialize Nerdio Manager (typical):

1. Open the Nerdio Manager URL from the App Service by selecting either the **Browse** button or the domain link in the **Overview** area.
2. Select the copy button to copy the command.
3. Select **Launch Azure Cloud Shell**, and then sign in as the **Global Administrator**, or **Privileged Role Administrator** combined with **Cloud Application Administrator**, and the subscription **Owner**.
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 is completed, you are returned to the prompt. The message **Deployment completed successfully** is displayed.

Note

If the installation was performed via the Marketplace or updated via the Automation Account, the message **NMW-After-Publish <Resource Group Name> <App Service Name>** is displayed.

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](#).

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 settings

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

When you navigate to the URL, you'll see a window with the following information shown:

Welcome to Nerdio Manager for Enterprise

Entra ID Tenant

Tenant: Nerdio Partner Solutions CustomerC - nerdiouniversity.net

ID:

Azure subscription

Name: PREVIEW NME - INTERNAL USE ONLY

ID:

Register Nerdio Manager

To configure the Nerdio Manager settings:

1. In the **Nerdio Manager registration** section:
 - Select **Register Nerdio Manager**.

- Enter your registration information.
 - Once you have entered all your registration information, select **Register**.
2. In the **Feature set** section, select your desired feature set:
 - Azure Virtual Desktop
 - Windows 365 (Cloud PCs)
 - Intune (Physical endpoints)

 Note

You can set up one, two, or all feature sets at the same time.

Selecting **Azure Virtual Desktop** exposes three configuration options: **Network**, **Directory**, and **File Storage**.

1. In the **Network** section:
 - Select **none selected**.
 - **Subnet**: From the drop-down list, select the subnet.
 - Select **OK**.
2. 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 Entra ID information.
 - Once you have entered all the desired information, select **OK**.
3. 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

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.

For more information about FSLogix Cloud Cache, see [Cloud Cache Overview](#).

- **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](#).

- **Manage App Service settings:** Select this option to edit the FSLogix App Service registry settings.
- **Manage Log settings:** Select this option to edit the FSLogix log registry settings.
- **FSLogix Profiles path (VHDLocation):** From the drop-down list, select an Azure Files share or Azure NetApp Files volumes. Alternatively, enter 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**.
4. Optionally, enable **Windows 365 & Intune**, and then configure the features and scopes:
 - Select **configure**.
 - Enable the required configuration features.
 - Select **OK**.

 Note

For details about 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 as a user with the Global Administrator role, then review and 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 **System > Settings > Nerdio**.

2. In the **Product edition** area, 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.

Activate your subscription

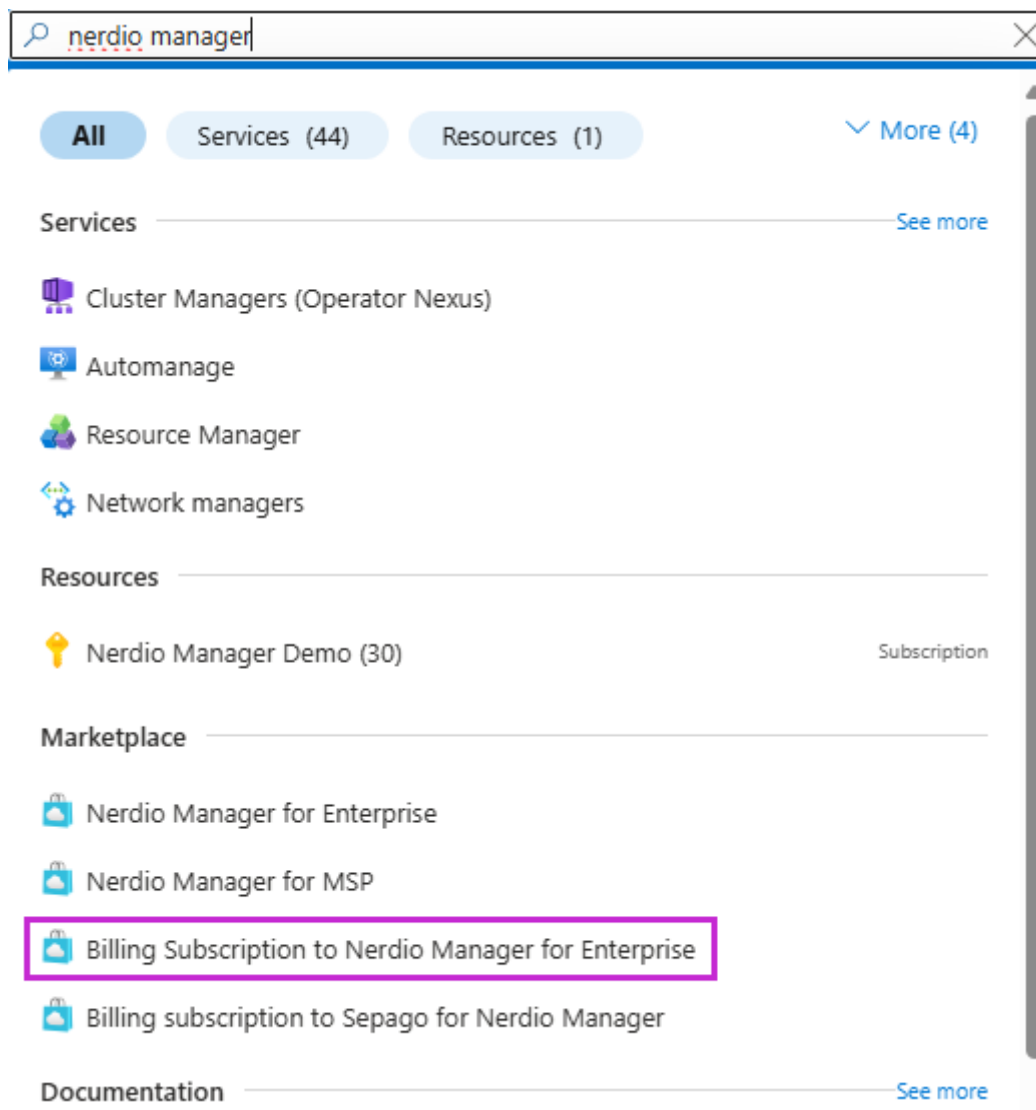
In order to continue using Nerdio Manager past the trial period, you must subscribe to our billing offer listed on the Azure Marketplace. This allows Nerdio Manager to report usage to Azure Marketplace. Based on your usage, you are charged for Nerdio Manager on your Azure bill from Microsoft.

Note

Activating your subscription also creates a new app registration in Entra ID. By default, this is named NerdioManagerForWVD-Subscribe. This application is granted Azure API permissions allowing you to authenticate and subscribe to the license. For more details, see [Azure Permissions and Nerdio Manager \(5\)](#).

To activate the Nerdio Manager subscription:

1. Sign in to your Azure portal as a **subscription owner** of the subscription where you plan to install the billing offer for Nerdio Manager from Azure Marketplace. The subscription you select can be different from the subscription where you installed Nerdio Manager for Enterprise.
2. In the search box, enter **Nerdio Manager**.
3. In the **Marketplace** section of the search results, select the **Billing subscription to Nerdio Manager Enterprise** option.



4. Enter the following information:

Note

You may see the **Price/payment frequency** list a \$0.00/month price plus a **Monthly Active Users** charge of \$3 /user/month. Further, the **Subtotal** shows \$0.00 for 1 month. You can safely ignore this portion; the charges listed in **Price/payment frequency** are for our internal billing system. Your pricing is based on whether you sign up for the Core edition or Premium edition as detailed in the Plan portion on the same screen. Continue the process and a subsequent page gives you the option to sign up for the edition of your choosing.

Plan details

Subscription * ⓘ	Microsoft Azure
Resource group * ⓘ	(New) Create new
Resource group location *	East US
Name * ⓘ	

- **Subscription:** From the drop-down list, select the subscription.
 - **Resource group:** Select **Create new** to create a new resource group.
 - **Resource group location:** From the drop-down list, select the resource group's region.
 - **Name:** Enter **BillingForNerdioManager**.
5. Once you have entered all the required information, select **Review + subscribe**.
 6. Review the **Terms of Use**.
 7. Select **Subscribe**.

The offer deployment starts. It takes about 2-3 minutes to complete. A **Subscription is in progress** message is displayed.

8. Once the deployment is complete, select **Configure account now**.
9. Select the installs you want to start billing for.

 Note

You generally have only one install of Nerdio Manager, so you see one item listed.

Billing is based on Monthly Active Users (MAUs). MAUs are the number of unique users that connected to an AVD desktop during the past month or are assigned to Windows 365 Enterprise Cloud PC at any given time in the past month.

Select to confirm	Subscription	Install ID ⓘ
☐	236b95399cae	b633
☐	236b95399cae	fc98f



10. Once you have selected all the installs, select **Subscribe**.

You have now subscribed to the billing offer and your Nerdio Manager license has been activated.

 Note

It is important for recurring billing to be left as **On**, which is the default.

Azure Environment: linked networks and resource groups

Nerdio Manager allows you to select or create virtual networks to use when adding desktop images, host pools, and session hosts. The Azure region of a given network determines the location of any VM created in that network.

You can also link resource groups that may contain session host VMs and desktop images.

Note

You can also set the default network and resource group for Nerdio Manager to use when creating a new desktop image, host pool, or session host. You can override these defaults during the creation process.

Manage linked networks

Nerdio Manager allows you to link, unlink, and create networks for use in creating new desktop images, host pools, and session hosts.

To link an existing network:

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked networks** area, select **Link Azure Network** or **Link Azure Local Network**.
3. From the drop-down list, select the subnet(s) you want to link.
4. Select **OK**.

You have made the specified network(s) available for use when creating new desktop images, host pools, and session hosts.

To create and link a new network:

Note

- For a deeper dive into the parameters and settings available for your network, see the Microsoft Learn article [Create, change, or delete a virtual network](#).
- Some of the optional configuration objects that you can create alongside the network may require further editing in the Azure portal.

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked networks** area, select **Create Azure Network**.
3. Enter the following information:
 - **Resource group:** Select the Azure resource group you want the network to use from the drop-down list.
 - **Region:** Select an available region from the drop-down list. VMs that use this network will be created in the network you select.
 - **Virtual network name:** Enter a display name for the virtual network.
 - **Enable IPv6:** Choose whether the virtual network will support IPv6 addressing.
 - **IP Range:** Use [CIDR notation](#) to enter an IP address range in either the IPv4 or IPv6 address space, depending on whether your network supports IPv6.
 - **Subnet Name:** Enter a subnet display name.
 - **Subnet:** Specify a subnet address in the range you specified above.
 - **Enable private subnet:** Choose this setting to disable default outbound access and require outbound internet access to be explicitly granted to VMs on the network.

 Note

On September 30, 2025, default outbound access for new deployments will be retired. For more information, see the [official announcement](#), and Microsoft's [guidance](#) on transitioning from default outbound access to an explicit method of public connectivity. We recommend that you use a NAT gateway (see below) to provide outbound internet access to the network.

- **NAT Gateway:** Select an existing NAT gateway from the drop-down list, or enter a name to create a new one. The NAT gateway will be created along with the network.
- **Network Security Group:** Optionally, select a [network security group](#) from the drop-down list to associate it with the network, or enter a name to create a new one. The network security group will be created along with the network.

- **Route Table:** Optionally, select a [route table](#) from the drop-down list to associate it with the network, or enter a name to create a new one. The route table will be created along with the network.
 - **Custom tags:** Optionally, enter the names and values of any custom metadata tags you want to associate with the network.
4. Click **OK**. The network and any associated configuration objects are created.

To unlink a network:

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked networks** area, locate the network you want to unlink.
3. In the **Actions** column, select the **Unlink** icon .
4. When prompted, select **OK** to confirm the operation.

Note

Resources deleted in the Azure portal outside of Nerdio Manager do not prevent unlinking of certain networks. Unlinking can be forced even if there are "orphan" objects that still refer to the network.

To set the default network:

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked networks** area, locate the network you want to make the default.
3. In the **Actions** column, select the **Set as default** icon .

Manage linked resource groups

Nerdio Manager allows you to link, unlink, and create resource groups for use in creating new desktop images, host pools, and session hosts.

To link a resource group:

1. Navigate to **System > Settings > Azure**.
2. In the **Linked resource groups** area, select **Link**.

3. From the drop-down list, select the resource group(s) you want to link.
4. Select **OK**.

You have made the specified resource group(s) available for use when creating new desktop images, host pools, and session hosts.

To unlink a resource group:

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked resource groups** area, locate the resource group you want to unlink.
3. In the **Actions** column, select the **Unlink** icon .
4. When prompted, select **OK** to confirm the operation.

Note

Resources deleted in the Azure portal outside of Nerdio Manager do not prevent unlinking of certain resource groups. Unlinking can be forced even if there are "orphan" objects that still refer to the resource group.

To set the default resource group:

1. Navigate to **System > Settings > Azure** blade.
2. In the **Linked resource groups** area, locate the resource group you want to make the default.
3. In the **Actions** column, select the **Set as default** icon .

User interface (UI) overview

Nerdio Manager's UI is feature rich and customizable. When you sign in, you will see the home page, showing your configured workspaces.

Time zone

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

Left-hand navigation pane

From the left hand navigation pane, you can select the component that you want to configure. For example, components such as **Endpoints**, or **Settings**.

Some components also have a sub-menu that can be accessed by selecting the down arrow. The additional options are then displayed.

To aid your navigation through the different menu levels, a breadcrumb trail is created so that you can easily return to an earlier page in your navigation flow.

Top menu icons

In the top-right of the UI, there are a number of icons that perform the following tasks:

Global search

Select the search  icon to search for a subject within the UI and enter the text you wish to search for. Matching subjects are displayed along with a link you can select to take you to that page in the UI.

Dark and light mode

The UI can be displayed with a dark background or a light background.

In light mode, select the dark mode  icon to switch to the dark background and once in dark mode, and you want to switch back to light mode, select the light mode  icon.

Notifications

Select the notification  icon to display any system notifications.

Announcements

Select the announcements icon  to display announcements. You can also review any announcements that have previously been dismissed.

Select the envelope  icon to mark the announcement as read, or select the eye  icon to view more details about the selected announcement.

Patent

Select the patent  icon to take you to the Nerdio intellectual property page on the Nerdio website.

Nerdio Manager Copilot

Select the Copilot  icon to launch the AI-assisted help system. For more details, see [Manage Nerdio Manager Copilot \(31\)](#).

Knowledgebase

Select the question mark  icon to take you to the Nerdio knowledgebase pages on the Nerdio website.

Sign out

To sign out of Nerdio Manager, select the down arrow next to the name of the currently signed in user, and then select **Sign out**.

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

Within some of the configurable components there is a **Tasks** area. This displays a log of the tasks related to the component you are configuring, in reverse chronological order. For example, the Workspaces page displays the log of the tasks performed on the Workspaces

Tasks, and the number of tasks, are color coordinated with those in green showing successfully completed tasks, those in red showing those tasks that have failed, and yellow showing those tasks that have been canceled. Tasks highlighted by the refresh  icon, are those tasks that have been created today and are currently in progress.

Task filtering

You can filter tasks by their status. Select  , and then from the **Filter by task status** drop-down list, select the status.

If you want to see more details about a particular task, select the information  icon, next to the task.

You can hide a task from the list by selecting the hide  icon.

For a task that is currently in progress, select the cancel  icon to cancel the task.

Task exporting

You can export the task logs to either a JSON file, or a CSV file.

Select  to export the task logs as a JSON file.

Select  to export the tasks logs as a CSV file.

The files are downloaded to the downloads folder of your browser.

For more details, see [Logs Module](#).

More actions menu

Several pages have additional menu options available in the more actions menu. Select the more actions  icon to access these menu options.

You also have access to additional menu actions by selecting the down arrow.

Search and filter

Many pages have search and filter features that allow you to quickly find the information you are looking for.

**Note**

You can also use the 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.

Refresh

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

Tool tips

Select the tool tip  icon to display 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.

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. For example, shown below, 3 session hosts have been selected. individually. You can now 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. You can also select all hosts by selecting the top-level box, next to the **Name** column.

Custom views

Nerdio Manager allows administrators to create custom views that best represents their specific 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. With custom views, you can combine similar data on a single page across the environment.

For more details, see [Create a Custom View](#).

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 so as not to have to create the filter each time.

For more details, see [Create a Custom View from an Existing Page](#).

Individualize your UI Themes

Nerdio Manager allows you to individualize your UI themes.

For more details, see [Individualize Your UI Themes](#).

Manage Nerdio Copilot

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



Note

Availability of Azure OpenAI services is limited and varies by Azure region.

Enable Nerdio Copilot

❗ Important

Nerdio Copilot has been completely rebuilt and refactored in NME 8.0. If you have previously deployed Nerdio Copilot, in NME 7.7 or previous versions, you will need to disable the legacy version Nerdio Copilot.

To uninstall the legacy version of Nerdio Copilot:

1. In Nerdio Manager, navigate to **System > Settings > Nerdio**.
2. Scroll down and expand the **Nerdio Manager Copilot** section.
3. Select **Configure**.

This will show all the resources that supported the legacy version of Nerdio Copilot.

4. Select **OK** to remove these resources.

To enable Nerdio Copilot:

1. In Nerdio Manager, navigate to **System > Settings > Nerdio**.
2. Scroll down and expand the **Nerdio Manager Copilot** section.
3. Select **Enabled**.
4. Enter the following information:
 - **Resource group**: From the drop-down list, select the resource group to which you want to assign all the resources required to run Nerdio Manager Copilot.
 - **Model**: From the drop-down lists, select the OpenAI model based on available quotas.
 - **Deployment type**: Choose deployment type. Either Data Zone Standard or Global Standard.
5. Once you have entered all the desired information, select **OK**.

The deployment task starts and takes about 2-5 minutes depending on the Azure region and other conditions. You can follow the task's progress in the **Tasks** section.

Use Nerdio Copilot

Once you've deployed all the required Azure resources, you can use Nerdio Copilot to help navigate Nerdio Manager.



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 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. Ask any question related to Nerdio Manager and send them to Copilot. After a short period of time, Copilot will display an answer.
3. Optionally, select **Citations** to view a list of cited Knowledge Base articles.
4. You may select either the sidebar window or detached window view options.

Manage Nerdio Copilot's chat settings

You may adjust Nerdio Copilot's settings at any time.

To manage Nerdio Copilot's chat settings:

1. Select the **Settings**  icon.
2. Enter the following information:
 - **Intent recognition service OpenAI Model:** From the drop-down list, select the desired model.
 - **Max days to retain history:** Enter the number of chat histories to retain.
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. For more details, see [Introduction to large language models](#).

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

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

Disable Nerdio Copilot

Follow this procedure to disable Nerdio Copilot.

Note

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

To disable Nerdio Copilot:

1. In Nerdio Manager, navigate to **System > Settings > Nerdio**.
2. Scroll down and expand the **Nerdio Manager Copilot** section, and select **Configure**.
3. When prompted, select **OK**.

The disable task starts and takes about 2-3 minutes depending on the Azure region and other conditions. You can follow the task's progress in the **Tasks** section.

Build scripts with Nerdio Copilot

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

⚠ Warning

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

To build a script with Nerdio Copilot:

1. Open Nerdio 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 t
[HKEY_LOCAL_MACHINE\SOFTWARE\MyApp]"NewFeatureEnable"=dword:1
```

3. Follow the prompts and reply as needed.
4. When the script is generated, copy the code.

Generate KQL queries with Nerdio Copilot AnalyticsPro

AnalyticsPro, is a powerful tool within Nerdio 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 Copilot.
2. Enter the details of the KQL query you want to generate. For example:

```
Can you write me a KQL query to get the number of active users from th
```

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

The cost of the feature depends on its usage. The cost is per tokens used, with costs varying depending on which model is chosen and how much it is used.

If the feature is enabled but not used, there is no standing cost.

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, Nerdio 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; this 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.

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** area.
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**.

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. 
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** area, from the drop-down list, select the schedule entry you wish to change or remove.
6. Once you have made the desired changes, select **Save**.

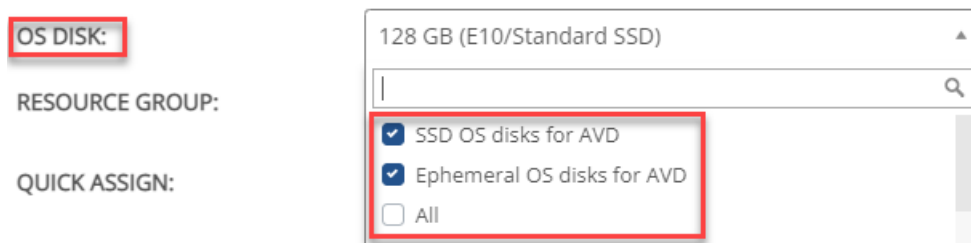
Resource Selection Rules Management

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.

 Note

- **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.

Step #2: Desktop Images

Once Nerdio Manager is installed, the next step is to prepare the desktop images your host pools will be built from - whether you're importing existing images or letting Nerdio Manager manage new ones for you.

In this section:

1. [Desktop Images \(43\)](#)
2. [Management and lifecycle tasks for imported desktop images \(44\)](#)
3. [Create a Desktop Image \(46\)](#)
4. [Desktop images: set as image \(55\)](#)
5. [Desktop Images Scripted Actions \(62\)](#)

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 \(64\)](#) 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. 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.

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

The typical desktop image lifecycle is as follows:

1. Import the desktop image.

See any of the following for detailed information:

- [Import images from the Azure library](#)
- [Import Custom Azure Managed Images](#)
- [Import an Existing VM](#)

2. Power on the desktop image:

- a. Navigate to **Cloud Desktops > Desktop Images**.
- b. Locate the desktop image you wish to power on.
- c. Select **Power 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 \(55\)](#) 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](#) 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.

For details, see:

- [Create dynamic host pools \(67\)](#)
- [Create static host pools without auto-scaling](#)
- [Resize/re-image a host pool](#)

Endpoint management software integration

Nerdio Manager allows you to use 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.

Example of endpoint management software integration

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 \(55\)](#) 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](#) 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.

Create a Desktop Image

Nerdio Manager for Enterprise allows you to create a desktop image either from an existing image in the Azure library or by importing an existing Azure VM.

Open the Create Desktop Image Wizard

1. Navigate to **Cloud Desktops > Desktop Images**.
2. From the bottom-right of the page, select **Create**.

The **Create Desktop Image** dialog opens. It contains the following sections: **VM**, **Join to AD**, **Settings**, **Clean up**, **Scripted Actions & Apps**, **Image**, **Replication**, and **Tags**.

Configure the VM

1. Refer to the table that matches the source of your desktop image, and enter the information listed.

 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 \(38\)](#) for details.

Azure library

UI Element	Type	Description
Source	Drop-down list	From the drop-down list, select Azure library to create the image from an existing image in your library.
Name	Text field	Enter the desktop image's name.
Description	Text field	Enter the description.
Network	Drop-down list	Select the network to which the VM connects. The VM is created in the Azure region associated with the network.
Azure image	Drop-down list	Select the desired image based on your Windows OS requirements, as supported by AVD, for example Windows 11 EVD Multi-Session (EVD = Enterprise Virtual Desktop). Images labeled Microsoft 365 Apps include a pre-installed version of Microsoft 365 Apps for enterprise, activated when licensed users sign in to the desktop. The list contains all standard Azure Marketplace images as well as all custom managed images available inside your Azure subscription.
Use the "staged" image version	Toggle	If enabled, this desktop image will be created using the "staged" image version of the selected desktop image, if one is available. This setting is only available for desktop images with Geographic distribution & Azure compute gallery enabled.
VM size	Drop-down list	Select the size.
OS disk	Drop-down list	Select the disk. You can also select the performance tier.
Resource group	Drop-down list	Select the resource group to contain the network interface cards of the VM.
Optimize disk type when desktop image is stopped	Checkbox	Downgrades the OS disk type when the desktop image is stopped in order to save money. When the VM starts, the OS disk type is changed back to the selected one.

Azure VM

UI Element	Type	Description
Source	Drop-down list	From the drop-down list, select Azure VM to import an existing VM as the desktop image.
SAS URL	Text field	Paste the SAS URL generated from the Azure portal. Your VM needs to be based on a Managed Disk: in the Azure portal, stop the VM, go to its OS disk, and select Disk Export to generate the URL.
Name	Text field	Enter the desktop image's name.
Description	Text field	Enter the description.
Network	Drop-down list	Select the network to which the VM connects. The VM is created in the Azure region associated with the network.
OS	Drop-down list	Select the operating system of the VM. If the selected OS requires Hyper-V Generation 2 (for example, Windows 11) and Gen2 is not yet enabled, a message displays prompting you to enable Create image VM as Gen2 on the Settings step, or to choose a Gen1-compatible image instead.
VM size	Drop-down list	Select the size.
OS disk	Drop-down list	Select the disk. You can also select the performance tier.
Resource group	Drop-down list	Select the resource group to contain the network interface cards of the VM.
Optimize disk type when desktop image is stopped	Checkbox	Downgrades the OS disk type when the desktop image is stopped in order to save money. When the VM starts, the OS disk type is changed back to the selected one.

2. Select **Next**.

Configure Join to AD

1. Configure the following:
 - **Join to AD**: Enabled by default. 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 in the **Custom credentials** field on the **Settings** step, since the VM won't be a member of the AD domain.
 - From the drop-down list, select the Active Directory domain to join, for example **denver.int (default)**.
2. Select **Next**.

Configure Settings

1. Enter the following information:

UI Element	Type	Description
Hibernation supported	Checkbox	Select this option if you want to allow the VM to hibernate. Hibernation provides the ability to deallocate your virtual machine while persisting the memory contents, allowing you to resume from where you left off the next time you start your VM. Hibernation cannot be enabled or disabled after the image is created.
Specialized image	Checkbox	Select this option if the image is a specialized image. Generalized images have had machine and user-specific information removed by running a command on the VM. Specialized images retain this information and have not gone through the generalization process.
Run sysprep in	Drop-down list	Select the context in which Sysprep should run on the VM, for example System-context.
Create image VM as Gen2	Checkbox	Available only when Azure VM is selected as the source on the VM step. Select this option to create the VM as Gen2. By default, desktop image VMs are created as Gen1. If the selected OS requires Gen2 and this option is not selected, a message displays prompting you to choose a Gen1-compatible Azure image to continue. See Support for Generation 2 VMs on Azure for details.
Time zone redirection	Checkbox	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	Toggle	Toggle this option On to set the time zone of the VM, then, from the drop-down list, select the time zone.
Boot diagnostics	Toggle	Enabled by default. Collects and stores diagnostic logs and screenshots while the VM boots.
Boot diagnostic storage account	Drop-down list	Applies only if Boot diagnostics is enabled. Leave this field set to Managed Storage Account (recommended) to store boot diagnostic logs in an Azure-managed storage account, or select a user-managed storage account from the list.

UI Element	Type	Description
Security type	Drop-down list	Select the security option that best suits your desktop image VM. Standard is set by default. Additional security options are only available for generation 2 VMs with Geographic distribution & Azure compute gallery enabled. Trusted launch and Confidential virtual machines improve security but have some limitations, such as lack of support for backup, managed disks, and ephemeral OS disks. See Trusted launch for Azure virtual machines and About Azure confidential VMs for details.
Secure Boot	Checkbox	Available only when Trusted launch virtual machines is selected as the Security type. Enables Secure Boot, which helps protect your VMs against boot kits, root-kits, and kernel-level malware.
vTPM	Checkbox	Available only when Trusted launch virtual machines is selected as the Security type. Enables 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	Checkbox	Available only when Trusted launch virtual machines is selected as the Security type. Enables 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.
Encryption at host	Toggle	Disabled by default. Provides end-to-end encryption for your VM data at rest and in transit, starting with the Azure hosts.
Custom credentials	Toggle	Disabled by default. Toggle On to enter the admin username and password for a local administrator user.
Install App Attach certificates	Checkbox	Select this option to install all the stored certificates on the VM, if applicable. To view the stored certificates, navigate to App Attach > Certificates.
Enable App-V client service	Checkbox	Select this option if the VM will use App Attach packages that contain App-V packages.

2. Select **Next**.

Configure Clean Up Options

1. Refer to the table that matches the source of your desktop image, and enter the information listed.

Azure library

UI Element	Type	Description
Skip removal of local profiles	Checkbox	Select this option to bypass this step and not remove local user profiles before running Sysprep. 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.
Uninstall legacy VDI agents	Checkbox	Select this option to attempt to remove Citrix and Omnicast VDI agents from the VM before capturing the image. Only detected agents are removed.
Remove FSLogix apps	Checkbox	Selected by default. Select this option to remove the FSLogix agent if it's found on the image. The FSLogix agent is not required on the desktop image: the latest FSLogix agent will be installed automatically on session hosts that are created from this desktop image.

Azure VM

UI Element	Type	Description
Skip removal of local profiles	Checkbox	Select this option to bypass this step and not remove local user profiles before running Sysprep. 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.
Uninstall legacy VDI agents	Checkbox	Select this option to attempt to remove Citrix and Omnicast VDI agents from the VM before capturing the image. Only detected agents are removed.
Uninstall FSLogix app	Checkbox	Selected by default. Use this option if 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	Checkbox	Use this option if you're creating an image from an existing AVD session host where the AVD agent has been previously installed. Be sure to uninstall the AVD agent before you set this imported VM as a desktop image. See Desktop Images Manually Uninstall AVD Agent for details.

2. Select **Next**.

Configure Scripted Actions and Applications

1. Enter the following information:

- **Run the following scripted actions:** Toggle this option **On**, then from the drop-down list, select the scripted action to run during creation.

Note

- 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 sysprepped. 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.
- **Pass AD credentials:** Select this option to pass AD credentials that are specified on the **Settings > Integrations > Active Directory** page to the scripts being executed. In the script, reference them as **\$ADUsername** and **\$ADPassword**.
 - **Target VM:** Select whether the scripted action runs against the **Clone** of the desktop image VM (default) or the **Source** VM.
 - **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.

Note

- 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.

- Select one of the following for the added application or application group:
 - **Install app**: Installs the selected application.
 - **Uninstall app**: Uninstalls the selected application.
 - **Install group**: Installs the selected application group.
 - **Uninstall group**: Uninstalls the selected application group.
- In the **Search application** field, select the app or application group to install or uninstall, based on the option selected above.
- **Show favorites only**: Select this option to display only those applications that are marked as favorites. Otherwise, you may search the list of applications.
- **Reboot after installation**: Select this option to reboot the clone of the desktop image VM after this application is installed. Subsequent application tasks will resume once the reboot is complete.
- **Target VM**: Select whether the application action runs against the **Clone** of the desktop image VM (default) or the **Source** VM.

2. Select **Next**.

Configure the Image

1. Enter the following information:

UI Element	Type	Description
Do not create image object	Checkbox	Select this option to create only a desktop image VM but not an image object. 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.
Geographic distribution & Azure compute gallery	Toggle	Enabled by default. Stores the image in an Azure Compute Gallery and automatically distributes it to the selected Azure regions.
Azure compute gallery	Text field / drop-down list	Type a name to select an existing Azure compute gallery or create a new one. Only one Azure Compute Gallery can be selected. The existing gallery must be in a linked resource group in the same Azure subscription as the image VM.

UI Element	Type	Description
Azure regions	Multi-select	Automatically populates with the region associated with the selected gallery. You can remove or add regions where the Desktop Image version should be replicated. The current Azure region must be part of the selection.
Replica count (per region)	Text field	Specify the number of replicas per region. Azure Compute Gallery replicas support a maximum of 20 concurrent clone operations per replica. Up to 100 replicas per region are supported. Replicas can only be deployed within the same subscription.

2. Select **Next**.

Configure Replication

1. Enter the following information:
 - **Enable for Cloud PCs:** Requires Windows 10/11 Enterprise. Not available for AVD, EVD, or CIS images.
 - **Custom (Azure local) locations:** From the drop-down list, select any custom Azure local locations to replicate the image to.
 - **Nutanix cluster** (AVD Hybrid on Nutanix AHV only): From the drop-down list, select the Nutanix cluster where the image should be synchronized.

Note

Only managed image versions (Active or Staged) are synchronized to Nutanix. Unmanaged (backup) versions are not synchronized. For more details, see [Create a VM Template for Nutanix Host Pools](#).

2. Select **Next**.

Configure Tags and Submit

1. Enter the following information:

 Note

You can specify multiple tags. The specified tags are applied to image VM, OS disk, network interface, image object, and Azure Compute Gallery image. For details about using tags to organize your Azure resources, see [Use tags to organize your Azure resources and management hierarchy](#).

- **Tag groups:** Optionally, select a predefined tag group from the drop-down list to apply its tags automatically.
- **Name** and **Value:** Optionally, enter a custom tag name and value.

2. Select **Submit**.

Nerdio Manager for Enterprise begins creating the desktop image. This may take up to an hour to complete. You can monitor progress on the **Tasks** tab of the **Desktop Images** page.

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 **Cloud Desktops > 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:

Nutanix cluster: (AVD Hybrid on Nutanix AHV only): From the drop-down list, select the Nutanix cluster where the image should be synchronized.

 Note

Only managed image versions (**Active** or **Staged**) are synchronized to Nutanix. Unmanaged (backup) versions are not synchronized. For more details, see [Create a VM Template for Nutanix Host Pools](#).

- **Run the following scripted actions before set as image:** Toggle this option **On** 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 list, 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.

 Note

- You may add as many applications as you need.
 - 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 clone of the desktop image VM after this application is installed. Subsequent application tasks will resume once the reboot is complete.

- **Show favorites only:** Select this option to display only those applications that are marked as favorites. Otherwise, you may search the list of applications.
- **Schedule:** Toggle the **Schedule** option **On** to perform the operations at a selected time(s). See [Manage Schedules for Tasks \(36\)](#) for details about creating a schedule.
- **Refresh image from Azure Marketplace:** Toggle this option **On** to remove the existing image object and replace it with the latest version of the selected Azure Marketplace image.

 Note

Enabling this option removes the existing desktop image VM and re-creates it from the latest version of the selected Azure Marketplace image.

- **Security type:** This option is locked based on the selection made when the image was created or imported into Nerdio Manager.

 Note

- **Standard** is set by default. Additional security options are available only 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 VMs. 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](#)

- **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:** This option is locked based on the selection made when the image was created or imported into Nerdio Manager.

 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.

- **Version Increment Type:** From the drop-down list, select one of the following options:
 - **Major**
 - **Minor**
 - **Revision**

 Note

Version numbers are in the format **Major.Minor.Revision**. For example, when updating version 1.4.3, the up-level version would be numbered as follows, depending on the option you choose in the **Version Increment Type** dropdown:

- **Major:** 2.0.0
- **Minor:** 1.5.0
- **Revision:** 1.4.4.

- **Specialized image:** Select this option if the image is a specialized image.

 Note

Generalized images have had machine and user-specific information removed by running a command on the VM. Specialized images retain this information and have not gone through the generalization process.

- **Hibernation supported:** Select this option if you want to allow the VM to hibernate.

 Note

Hibernation provides the ability to deallocate your virtual machine while persisting the memory contents. This allows you to resume from where you left off the next time you start your VM. Note that hibernation cannot be enabled or disabled after the image is created.

- **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](#) for details about activating staged desktop images.

- **Activate staged image after:** Select this option to automatically activate the image a number of days after staging. Any linked pools will have their associated image updated.
- **Current image action:** Select one of the following:
 - **Keep current version as backup:** This option retains 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. You can still use prior versions of Azure Compute Gallery images in the **Desktop image (template)** menu, under **Unmanaged ACG image versions**.

- **Remove current version after activation:** This option removes the current image version automatically after activation.
- **Replica Count (Per Region):** Specify the 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 can only be deployed within the same subscription.

- **Backup Version Limit:** Specify the maximum number of backup image versions that can be retained.

 Note

When a new image version is created, and the old one is saved as a backup, the system automatically manages and limits the number of these backups according to the specified limit. If the limit is reached, the oldest versions are deleted. You can configure this setting in the desktop image settings, **Manage versions** option.

- **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 the Azure portal > **Images**. In Nerdio Manager's image selector lists, it is listed under **Custom images**.

- **Install App Attach certificates:** Select this option to install all stored certificates on the image VM, if any.
- **Enable App-V client service:** Select this option if the VM will use App Attach packages that contain App-V packages.
- **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.

- **Enable for Cloud PCs:** Select this option to make this image available in Windows 365 Cloud PC service.

 Note

The image will be uploaded and tested for compatibility with Cloud PCs. This process can take a long time. There is a limit of 20 images that can be uploaded to Windows 365.

- **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.
- **Apply tags:** Optionally, enter the **Name** and **Value** of the Azure tag.

 Note

You can specify multiple tags. The specified tags are applied to image VM, OS disk, network interface, image object, and Azure Compute Gallery image. For details about using tags to organize your Azure resources, see [Use tags to organize your Azure resources and management hierarchy](#).

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. For details about the logs, see [Desktop Images Change Log Feature](#).

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 \(36\)](#) 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.

Step #3: Host Pools

With your desktop images in place, the next step is to create host pools - the pools of session hosts your users will actually connect to - and configure how they're built, scaled, and assigned.

In this section:

1. [Overview of host pools \(64\)](#)
2. [Workspace Management \(66\)](#)
3. [Create dynamic host pools \(67\)](#)
4. [Manage host pool profiles \(75\)](#)
5. [Enable dynamic host pool Auto-scaling \(79\)](#)
6. [Enable personal host pool Auto-scaling \(94\)](#)
7. [Auto-scale: Cost Optimization Session Host VM OS Disk Storage \(113\)](#)
8. [Add a new session host to a dynamic host pool \(114\)](#)
9. [Host Pool AVD Configuration \(118\)](#)
10. [Host pool VM deployment \(122\)](#)
11. [Manage Host Pool User Assignments \(131\)](#)
12. [Configure the Host Pool's Active Directory Settings \(131\)](#)
13. [Start VM on Connect for Pooled Host Pools \(133\)](#)
14. [Configure User Session Time Limits \(133\)](#)
15. [Publish remote applications to users \(137\)](#)

Overview of 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.

Host pools can be configured in the following ways:

Whether auto-scale is enabled:

- **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. Auto-scale can be enabled on a static host pool after creation, if needed.

 Note

When Nerdio Manager is first deployed to an **existing** environment, the host pools that are created are static. Auto-scale can be enabled on them afterward.

- **Auto-scale enabled:** Session hosts are created and removed automatically based on your auto-scale configuration, according to workload demand.

 Note

This was previously referred to as a "dynamic" host pool. You may still see this term in some parts of the product while this terminology transition is in progress.

Where session hosts run:

- **Azure:** Session hosts run entirely in Azure.
- **AVD Hybrid:** Session hosts run on infrastructure connected via Azure Virtual Desktop for Azure Local or Nutanix AHV.

See also

- [Create Static Host Pools Without Auto-Scaling](#)

- [Create Dynamic Host Pools \(67\)](#)
- [Delete Hosts, Host Pools, and Workspaces](#)
- [Convert a Static Host Pool to Dynamic](#)
- [AVD for Azure Local and Nerdio Manager](#)
- [AVD Hybrid Support](#)

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 **Cloud Desktops > Azure Virtual Desktop > 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:

- **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 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:



Note

Many fields in this wizard have an info tooltip alongside the field label. Reference these tooltips for more information about each option.

Open the Add Host Pool Wizard

1. Navigate to **Cloud Desktops > Azure Virtual Desktop > Workspaces**.
2. Select the workspace you wish to work with.
3. Select **New host pool**.

A dialog opens titled *Add Host Pool*. It contains the following sections: Basics, VM Template, Active Directory, FSLogix, RDP, Tags, Application policies.

Configure Basics

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 \(38\)](#) for details.

- **Name:** Enter the name of the host pool.
- **Description:** Enter 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.
- **Host type:** From the drop-down list, select the host type (Azure Cloud, Azure Local, or Nutanix).
- **Host pool type:** Select **Dynamic**.
- **Desktop Experience:** From the drop-down list, select the desktop experience.
 - **AVD multi-session 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.
 - **AVD multi-session 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.
 - **AVD single-session 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.
 - **AVD single-session desktop (personal):** This is a personal (persistent) full desktop experience. A dedicated session host VM is assigned to each user.
- When you select **AVD single-session desktop (personal)** as the **Desktop Experience**, you need to configure the following additional features:
 - **Assignment Type:** Select how the desktop is assigned to the user.

 Note

Before users can sign into a personal desktop, they need to be pre-assigned to the VM.

- Optionally, select **Assign multiple desktops to a single user**.

 Note

Selecting this option allows multiple desktops to be assigned to a single user for this host pool. This setting CANNOT be disabled after being enabled, and is only available for direct assignments. For more details, see [Configure personal desktop assignment](#).

- **App group name:** Optionally, enter the app group name of 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.
- **Quick Assign:** From the drop-down list, select the users or groups to pre-assign to newly created desktops.

Select **Next**.

Configure the VM Template

- **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.
 - **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.

Select **Next**.

Configure Active Directory

- **Directory profile:** From the drop-down list, select **Default**, one of the **Predefined** global configurations, or **Custom**.

Note

Default always uses the application's global default AD configuration, so it stays in sync if that default is later changed. Selecting a Predefined configuration locks in that specific saved configuration, even if the global default changes afterward. Select Custom to provide a configuration specific to this host pool.

- **Directory type, Domain (FQDN), Service account (UPN), Service account password, and Organization unit:** These fields are populated automatically from the selected directory profile and remain read-only unless **Custom** is selected for Directory profile, in which case they become editable. Specify the Organization unit as a Distinguished Name (DN) path if session hosts should be created in a specific OU; leave it blank to use the Computers container.

Select **Next**.

Configure FSLogix

- **FSLogix:** From the drop-down list, select the FSLogix configuration profile to be used when creating or re-imaging hosts in this host pool.
- **FSLogix Profiles:** Select the toggle to enable FSLogix profiles.

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.

- **Configuration:** From the drop-down list, select an existing profile, or select **Custom** to configure the settings below yourself.

 Note

Selecting an existing profile automatically completes the configuration with that profile's settings, which cannot be edited here. Selecting Custom lets you configure the profile as required.

- **Version:** From the drop-down list, select the FSLogix version.
- **Configure session hosts registry for Entra ID joined storage, Exclude the local admin accounts from FSLogix, and Exclude domain accounts from FSLogix:** Select any of these options as needed, and enter applicable domain accounts in the **Domain accounts** field.
- **FSLogix profiles path (VHDLocation):** Select **Override** to specify a custom profile storage location instead of the default.
- **Configure Office Container to redirect Microsoft Office user data (ODFC):** Select this option to redirect Office container data, and specify the **FSLogix Office Container path (VHDLocation)** if overriding the default.
- **FSLogix cloud cache:** Select the toggle to enable FSLogix Cloud Cache, which replicates profiles asynchronously across multiple storage locations for resiliency.

 Tip

For performance reasons, it is strongly recommended that you use Premium SSD and Ephemeral OS disks when Cloud Cache is enabled.

- **Manage App Service settings and Manage Log settings:** Select either option to edit the corresponding FSLogix registry settings.
- **FSLogix Registry Options:** From the **Edit mode** drop-down list, select **All settings** or **Advanced**, then configure individual registry values across the Profile Settings, ODFC Settings, Cloud Cache Settings, App Service Settings, and Log Settings tabs. Use the **Search settings by name** box to filter.

 Note

See [FSLogix per-host pool customization](#) for the full list of configurable registry settings.

Select **Next**.

Configure RDP

- **RDP Profile:** From the drop-down list, select the RDP profile.

Note

This step also includes RDP Shortpath network settings and, for a Custom profile, individual redirect and session options. See [Host Pool Custom RDP Configuration](#) for more information.

Select **Next**.

Configure Tags

- **Tag groups:** Optionally, from the drop-down list, select an existing tag group. Selecting a tag group auto-populates the Name and Value fields below with its predefined values.
- **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.

Select **Next**.

Complete the Wizard

- **Application policies:** Optionally, select the application policies to assign to the host pool.

**Note**

This step displays a notice that host pool creation runs as a background task.

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

You are redirected to the new host pool's auto-scale settings page. If desired, configure the auto-scaling for the host pool. See [Enable Dynamic Host Pool Auto-scaling \(79\)](#) 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 \(79\)](#)

[Host Pools \(64\)](#)

[Create Static Host Pools Without Auto-Scaling](#)

[Delete Hosts, Host Pools, and Workspaces](#)

Manage host pool profiles

Host pool profiles simplify the creation of new host pools by letting you define reusable profiles for auto-scale settings, FSlogix settings, RDP settings, and directory settings. When configuring any of these for a host pool, you can select a predefined profile. This eliminates the need for manual configuration for each pool or schedule.

**Note**

Auto-scale profiles are available only in the Nerdio Manager **Premium** edition.

Create a host pool profile

Complete the following steps to create a new host pool profile.

To create a profile:

1. Navigate to **Settings > Host Pool Profiles**.
2. In the **Profiles** area, select **New profile**.
3. Select the profile you wish to create:
 - **Auto-scale**: Enter the following information:
 - **Auto-scale mode**: From the drop-down list, select the auto-scale mode.

The following modes are available:

- **Shared**: For all pooled dynamic hosts pools.
- **Schedule-based (Personal)**: For single user desktop personal host pools with auto-scaling that is performed as per the specified schedule.
- **User-driven (Personal)**: For single user desktop personal host pools with auto-scaling that is performed when there are no active or disconnected sessions.
- **Name**: Enter the profile name.
- **Description**: Enter the profile description.
- For all the other parameters, see the relevant article:
 - For pooled dynamic host pools: [Enable Dynamic Host Pool Auto-scaling \(79\)](#).
 - For single user desktop personal host pools: [Enable Personal Host Pool Auto-scaling \(94\)](#).
- **Directory**: Complete the steps as described in [Configure the Host Pool's Active Directory Settings \(131\)](#).
- **RDP**: Complete the steps as described in [Configure RDP Settings Profiles](#).

- **FSLogix:** Complete the steps as described in [FSLogix settings and configuration \(174\)](#).

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

Assign a host pool profile

Once you created a host pool profile, you can assign it to relevant host pools.

To assign a profile to a host pool:

1. Navigate to **Settings > Host Pool Profiles**.
2. From the action menu, select **Assignments**, then **New assignments**.
3. Enter the following information:
 - **Auto-scale profile:** From the drop-down list, select the auto-scale profile.
 - **Schedule type:** From the drop-down list, select the schedule type.
 - **RDP profile:** From the drop-down list, select the RDP profile type.
 - **FSLogix profile:** From the drop-down list, select the FSLogix profile type.
 - **AD profile:** From the drop-down list, select the AD profile.
 - **Host pools:** From the drop-down list, select the host pool(s).
 - **Stop on first failure:** Each host pool is processed one at a time. Select this option to cancel the remaining operations on the first failure.

ADD HOST POOL PROFILE ASSIGNMENTS

Auto-scale profile: ✕ ▼ ⓘ

Schedule type: * ▼ ⓘ

RDP profile: ✕ ▼ ⓘ

FsLogix profile: ✕ ▼ ⓘ

AD profile: ✕ ▼ ⓘ

Host pools: * ✕ ✕ ▼ ⓘ

☐ Stop on first failure ⓘ

Cancel Save

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

 Note

You can perform the following on auto-scale profile assignments:

- **Edit selected Alternative:** Select this to edit an alternative schedule.
- **Remove selected:** Select this option to remove selected assignments.

Manage host pool profiles

You can manage existing host pool profiles.

To manage profiles:

1. Navigate to **Settings > Host Pool Profiles**.
2. Locate the host pool profile you wish to work with.

3. Select the from the following:

- Select the pencil  icon to edit the profile.
- Select the more actions  menu, for the following options:
 - **Assignments:** Edit the assignments.
 - **Set default:** Sets the profile as default.
 - **Clone:** Create a clone of the profile.
 - **Delete:** Delete the profile.

Compare host pool profiles

You can compare two existing host pool profiles.

To compare profiles:

- Select the profiles you want to compare.
- Select **Compare**.
- Optionally, select **Show only different** to display only the properties that differ between the two profiles. Select **Show all** to return to showing all properties, including those that are identical between the two profiles.

Directory Profiles Comparison

SETTING	AD_NME-QA-STANDARD-AD.LOCAL (DEFAULT)	ENTRAID_WITHOUT_INTUNE
Is Default	Yes	No
Directory Type	Active Directory	Entra ID
Friendly Name	AD_nme-qa-standard-ad.local	EntraID_Without_Intune
Domain	nme-qa-standard-ad.local	Not set
Username	nerdloadmin@nme-qa-standard-ad.local	Not set
Organization Unit		Not set
Enroll with Intune	Not set	No
Profile name	AD_nme-qa-standard-ad.local (default)	EntraID_Without_Intune

Show only different

Close

Enable dynamic host pool Auto-scaling

The Auto-scaling 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 Auto-scaling 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 more options  menu, hover over **Auto-scale**, and select **Configure**.
3. Enter the following basic auto-scale information:
 - **Auto-Scale**: Toggle this option to **Enabled**.
 - **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.

- **Additional subnets:** From the drop-down list, select additional subnets within the same virtual network.

 Note

If a particular subnet does not have enough IP addresses when scaling out, then the next subnet will be chosen automatically when creating additional session hosts.

- **Network distribution:** From the drop-down list, select how the load is distributed across the network.

 Note

Select **Depth first** to distribute the load to nodes one after another in a fixed order, or, for optimal distribution, select **Breadth first** to balance the load proportionally based on current resource usage.

- **Desktop Image (template):** From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **Use the "staged" image version:** Select this option to use the staged image version, if available, when scaling the host pool.
- **VM Size (template):** 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 \(113\)](#) 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:** Select one of the following options from the dropdown:
 - **Disabled:** No re-imaging takes place.
 - **Always:** Hosts that had at least one user signed in to them are re-imaged. For multi-session hosts, the hosts are re-imaged as soon as the last user signs out.
 - **During scale-in restrictions only:** Re-imaging occurs only within the configured scale-in restriction period, mitigating the risk of reduced session capacity on the host pool at other times.
 - **Scaling interval:** From the drop-down list, select the time interval.
 - **Schedule type:** Select the **Default schedule** or **Alternative schedule**.
 - 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** area to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, select **Alternative schedule**, 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 this option to **Enabled**.
- **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.
- 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

For more details, see [Manage Auto-scale Profiles \(75\)](#).

4. 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 VM on connect:** Select this option to start the session host VMs on connect.

5. 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.

6. 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. When enabled, you can configure the number of hosts in a group to scale out or scale in.



Note

The multiple auto-scale triggers feature is available only in the Nerdio Manager **Premium** edition.



Note

- 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 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 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.
7. Enter the following **Rolling Drain Mode** information:

 Note

- 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).
- If a VM is using ephemeral storage, it will be deactivated rather than stopped when scaled in using Rolling Drain Mode.

- **Rolling Drain Mode:** Toggle this option to **Enabled** 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

- **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.

8. 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. Use   to add or remove schedules.

 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.

9. 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.
- **Message content:** Enter the warning message text.

10. 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 to **Enabled** to enable auto-heal.
- **AVD agent status:** 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.

- **First action timeout:** Enter the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

 Note

- 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.

- **Timeout 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.

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

Related topics:

- [Create Dynamic Host Pools \(67\)](#)
- [Enable Personal Host Pool Auto-scaling \(94\)](#)

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 more options  menu, hover over **Auto-scale** , and select **Configure**.
3. At the bottom of the page, toggle **Auto-scale** to **Enabled**.
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.

- **Additional subnets:** From the drop-down list, select an additional subnet from the same virtual network.

 Note

When scaling out, if a particular subnet does not have enough IP addresses, the next subnet will be chosen automatically when creating additional session hosts.

- **Network distribution:** From the drop-down list, select how the network load should be distributed. Select either **Depth first**, or **Breadth first**.

 Note

Select **Depth first** to distribute network load to nodes one after another in a fixed order, or select **Breadth first** to balance the network load proportionally based on current resource usage.

- **Desktop image (template)**: From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **VM size (template)**: 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 **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 a holiday period when you have a large number of contingent users. In either case, you would use the **Alternative schedule** area to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, select the **Alternative schedule** area and enter the following information:
 - **Schedule:** Select the toggle to enable the alternative schedule.
 - **Days:** From the drop-down list, select the off-peak day(s).
 - **Dates:** Select the date field, and from the calendar that is displayed, select the date..
 - Select the plus  icon to add another date, or select the minus  icon to remove dates.
6. **Auto-scale mode:** From the drop-down list, select the desired auto-scale mode.

 Note

- **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:** 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 \(75\)](#) for details about creating and working with auto-scale profiles.

8. Continue the configuration process with the relevant auto-scale mode:
 - **User-driven:** [To enable user-driven personal host pool auto-scaling. \(98\)](#)
 - **Schedule-based:** [To enable schedule-based personal host pool auto-scaling. \(105\)](#)

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 VM 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 to enable desktop start and stop.
 - **Desktops are stopped after:** From the drop-down list, select the number of minutes or hours to scale in after all users have signed out.

 Note

- 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-stagehosts:** Toggle this option to enable pre-staging hosts.

 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:

 Note

For more details and examples of intelligent disk pre-staging, see [Intelligent disk pre-staging for personal host pools](#)

- **Pre-stage host OS Disks:** Toggle this option to enable pre-staging host 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:** When **Use intelligent disk pre-staging for users** is selected, from the **Mode** 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 to enable auto-grow.
- **Add a new host when the number of available (not assigned to a user) falls below:** Enter 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 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 time duration before a desktop is deleted..

 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 **System > Settings > Nerdio** 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:** 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 to enable auto-heal.
 - In the **Sign of a broken host** box, enter the following information:
 - **AVD agent status:** From the drop-down list, select the AVD agent status, and then from the drop-down lost below, select 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.

- **First action:** Enter the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

 Note

- 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.

- **Timeout 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.

- To add an addition Sign of a broken host, select the plus  icon.

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

To enable schedule-based personal host pool auto-scaling:

1. From the **Auto-scale mode** drop-down list, select **Schedule-based**.
2. From the **Auto-scale profile** drop-down list, select the auto scale profile.
3. Enter the following **Host pool properties** information:
 - **Start VM on connect:** Select this option to start the desktop on connect.
4. Enter the following **Working hours** information:
 - From the drop-down lists, select the **Work days** and **Working hours** 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.

5. 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:** If you have selected the **Use intelligent desktop pre-staging for users** option, then 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.

- **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 **System > Settings > Nerdio** 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.

8. 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.

9. 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 to enable auto-heal.
- **AVD agent status:** From the drop-down list, 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.

- **First action timeout:** Type the number of minutes to wait before running the first action.
- **Recovery actions:** From the drop-down list, select the recovery action(s).

 Note

- 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.

- **Timeout 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.

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

Related Topics

[Create Dynamic Host Pools \(67\)](#)[Enable Dynamic Host Pool Auto-scaling \(79\)](#)

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.

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 **Cloud Desktops > Azure Virtual Desktop > Workspaces > 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**.

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 \(79\)](#) 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. Do the following:

From the more options  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 \(38\)](#) for details.

- Select **Run now** or **Schedule**.
 - The **Schedule** area allows you to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **OK**. See [Manage Schedules for Tasks \(36\)](#) for details about creating a schedule. Select the schedule from the drop-down list, or create a new schedule.

Add Host to Dynamic Pool

No session hosts to process now

▶ Run now

 New schedule *

SCHEDULE

New 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. Select optional filters if required to show specific OS disk types. For example, select **All disks performance tiers** to show the premium SSD disks.

 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.

4. If you have entered a **Host Count** that is greater than 1, enter the following information:
 - **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.

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

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 **Settings > Virtual Machines**.
3. Enter the following information:
4. Enter the following **Operating System** options:
 - **Set time zone**: Enable this option, and from the drop-down list select the time zone, to set the time zone on the VM when it is provisioned.
 - **Time zone redirection**: Enable this option to allow users to see their local device's time zone inside of their session.
 - **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.

- **Automatically deallocate powered-off 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.
- **Boot diagnostics:** Enable 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

- **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.

 Note

Nerdio Manager honors the Azure default setting, which is Automatic by OS (Windows Automatic Updates).

- **Accelerated networking (if supported):** Enable 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.

- **NVMe (if supported):** Enable 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.

- **GPU drivers (if supported):** Enable this option to install either [NVIDIA](#) or [AMD](#) drivers.

 Note

GPU drivers can be installed on N-series VMs.

- **H.265 encoding (if supported):** Enable this option to enable H.265 High Efficiency Video Coding hardware acceleration.

 Note

H.265 hardware acceleration is available only on N-series VM sizes using NVidia GPUs.

- **Deploy VMs to Capacity reservation groups:** Enable 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).
- **Deploy VMs across availability zones:** Enable this option to automatically distribute newly created or re-imaged session host VMs across Availability Zones in the selected Azure region.

 Note

- To ensure that Nerdio Manager considers all possible availability zones when reinstantiating VMs, ensure that **Availability Zone Awareness** is turned on in [Host Pool Azure Capacity Extender Configuration](#).
- See this Microsoft [article](#) for more details about Azure Regions and Availability Zones.

- **Availability zone:** From the drop-down list, select the availability zone(s).
- **Deploy VMs on dedicated hosts:** Enable this option to deploy 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.

- **Deploy VMs in a proximity placement group:** Enable this option to deploy VMs in a proximity placement group.

 Note

VMs placed in a proximity group are located physically close to each other in an Azure data center, ensuring the lowest possible network latency between the VMs. See [Learn Microsoft: Proximity placement groups](#) for details.

- **Proximity placement group:** From the drop-down list, select the proximity placement group.

-

 Note

The selected group is automatically assigned to the VM at creation. If no suitable resource is found, VMs creation fails.

- **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.

- **Install App Attach certificates:** Select this option to install all stored certificates if the App Attach packages are added to this host pool.
- **App-v client service:** Enable this option to enable the App-V client service, which is required if the VM uses App Attach packages containing an App-V package.
- **Install Applications:** Enable this option to install applications configured by recurrent UAM policies before moving the host out of drain mode.
- **Entra ID group(s):** From the drop-down list, select the default Entra ID group(s) to add the session hosts to.
- **Entra connect replication timeout (minutes):** For hybrid enrollments, type a maximum delay for machine account replication from active directory via Entra Connect.

 Note

By default, this is 30 minutes. A value up to 120 minutes can be specified.

- **Enforce Intune compliance :** From the drop-down list, select this option to make hosts unavailable to users until the Intune compliance requirements are met.

 Note

- Optionally, select **Compliance policies only** or **All policies**. The **All policies** option also requires that Intune managed apps are installed successfully before the host is released from drain mode.
 - Intune integration must be enabled to make use of this feature, with the following options:
 - The **Compliance policies only** setting requires **Intune managed devices** read permissions.
 - The **All policies** setting additionally requires **Device Policies & App policies** read permissions.
 - Enabling either option may result in significant increase in provisioning time, depending on the configured Intune compliance requirements.
- **Allow non-admin users to shadow sessions:** Enable this option to allow 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.
- **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.

- **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.



Note

- 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.

- **Disk encryption sets:** From the drop-down list, select the disk encryption sets to be used to provide customer-managed key functionality.



Note

By default, Nerdio Manager uses platform-managed keys. To use the default setting, leave the disk encryption sets blank. If disk encryption sets are required, create these from the Azure portal, in the same region as the desktop pool. Available disk encryption sets can be selected from the drop-down list. To learn more about key options, see [Server-side encryption of Azure Disk Storage](#).

- **Application security group:** From the drop-down list, select the Application Security Groups (ASGs) that enable you to configure network security as a natural extension of an application's structure.

 Note

This allows you to group virtual machines and define network security policies based on those groups. This feature allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses. VMs with network interfaces in different regions than the ASG are created without ASG support. The maximum number of supported ASGs is 10.

See [Application Security Groups](#) for more information.

- **Watermarking:** Enable 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.
- **Scripts signing:** Enable this option to enable script signing.

 Note

Nerdio Manager can automatically sign all PowerShell extensions and scripted actions running on session host VMs using a specified signing certificate. Please note that the selected certificate must be installed on the VMs for the scripts to work.

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

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. From the action menu, select **Manage > Users and groups**.
3. Alternatively, in the **Status** column, select the number next to **Assigned users** to view the users and groups.
4. In the **Assignments** window, you may search, sort, and filter the users and groups. For example, filter for all users not assigned to the host pool.
5. To unassign users from the host pool, select the  icon next to the user(s) you wish to unassign.
6. When you have selected all the users, select **Unassign**.
7. To assign users to the host pool, select the  icon next to the user(s) you wish to assign.
8. When you have selected all the users, select **Assign**.

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

[Azure Active Directory - Definition of Terms](#)

[Configure Entra Domain Services for use with AVD](#)

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

Users are often moved to a cloud environment because one application no longer runs locally. However, there are great cost savings to be had by simply running one or more applications remotely. This guide walks you through the how's and why's of setting-up an AVD host Pool with remote applications.

You can use Nerdio Manager to easily publish applications (RemoteApps) within Azure Virtual Desktop. These applications may be restricted by application groups, if required, allowing administrators to publish different apps to different users from the same host pool.

What are Remote Applications?

Like the name suggests, RemoteApps are applications that are run remotely. However, despite what some people may think, remote apps require a multi-session AVD host to be able to utilize the application remotely. You install your applications just like you would with a traditional Remote Desktop solution. However, when you go to publish the application for remote users, you can choose which apps the user has access to. This is handled by Application Groups.



Note

If you have full-desktop experiences for users, instead of remote apps, you can limit the apps the users have access to with FSLogix App Masking.

Why RemoteApps?

RemoteApps are less resource-intensive than a full desktop experience, allowing you to have more users on a given host, thereby reducing costs.

What are Application Groups?

In Azure Virtual Desktop (AVD), application groups define what users can access, either a full desktop or specific apps, within a host pool. Users can be assigned to multiple application groups across different host pools for flexible access.

There are the following types:

- **Desktop:** Gives access to a full Windows desktop (pooled or personal host pools).
- **RemoteApp:** Provides access to selected apps (pooled host pools only).

You can assign both types to the same pooled host pool, but only one Desktop group per pool. Multiple RemoteApp groups can be assigned, and users see all apps from those groups.

If a user is assigned both Desktop and RemoteApp in the same pool, they'll only see the [preferred application group type](#), based on the pool's settings.

Configure your host pool

As mentioned previously, you need a multi-user host pool to utilize Remote Applications. Ideally, you should create a new host pool. However, if you already have an existing host pool, you can easily add a RemoteApp Group and/or switch to a RemoteApp group.

Provision your Desktop Image and Host(s)

Now that you have your host pool, you need to create or update your desktop image and then deploy it to your host pool. See [Desktop images: set as image \(55\)](#) for details.

Add application 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 more options  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.

You can publish RemoteApps using the following methods:

- [Publish a remote application installed on a host to users \(140\)](#)
- [Publish a remote application from an App Attach package to users \(142\)](#)
- [Publish a remote application from a file path to users \(143\)](#)

Publish a remote application installed on a host to users

Nerdio Manager enables you to deliver applications installed on a host, to your users.

To publish a remote application installed on a host to users:

1. Select the host pool you want to work with. This is a host pool configured for the **RemoteApp (Pooled)** desktop experience.
2. From the more options  menu, select **Applications > RemoteApps**.
3. Select **New RemoteApp**.

 Note

- 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. In the **Select App Group** dialog box, enter the following information:
 - From the drop-down list, select the app group.
 - Select **OK**.
5. In the **Publish Application** dialog box, enter the following information:
 - **Application Source**: From the drop-down list, select **Installed on host**.

 Note **Note**

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.
- **Command Line Setting:** Select this option to require a command line setting.
- **Command Line:** Type the command line to pass to the executable when launching the RemoteApp.

6. 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.

Publish a remote application from an App Attach package to users

Nerdio Manager enables you to deliver App Attach packaged applications to your users.

To publish a remote application from an App Attach package to users:

1. Select the host pool you want to work with. This is a host pool configured for the **RemoteApp (Pooled)** desktop experience.
2. From the more options  menu, select **Applications > RemoteApps**.
3. Select **New RemoteApp**.
4. In the **Select App Group** dialog box, enter the following information:
 - From the drop-down list, select the app group.
 - Select **OK**.
5. In the **Publish Application** dialog box, enter the following information:
 - **Application Source**: From the drop-down list, select **App Attach Package**.
 - **App Attach Package**: From the drop-down list, select the App Attach package.
 - **MSIX Application**: From the drop-down list, select the MSIX application.
 - **Friendly Name**: Optionally, type the friendly name that is visible to the user.
 - **Description**: Type the description that is visible to the admin.
 - **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.
6. Once you have entered the desired information, select **OK**.

Publish a remote application from a file path to users

Nerdio Manager enables you to deliver applications from a file path to your users.

To publish a remote application from a file path to users:

1. Select the host pool you want to work with. This is a host pool configured for the **RemoteApp (Pooled)** desktop experience.
2. From the more options  menu, select **Applications > RemoteApps**.
3. Select **New RemoteApp**.
4. In the **Select App Group** dialog box, enter the following information:
 - From the drop-down list, select the app group.
 - Select **OK**.
5. In the **Publish Application** dialog box, enter the following information:

- **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.
- **Command Line Setting:** Select this option to require a command line setting.
- **Command Line:** Type the command line to pass to the executable when launching the RemoteApp

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

Related Topics

[Remote Applications Maintenance Mode](#)

Step #4: Storage

Once your host pools are running, the next step is to configure storage for user data and profiles. Nerdio Manager works with both Azure Files and Azure NetApp Files: native Azure services commonly used in place of a dedicated file-server VM, and often paired with a profile management solution such as FSLogix.

You can link Nerdio Manager to an existing Azure Files or Azure NetApp Files share, or have Nerdio Manager create and configure a new one for you, including permissions and domain-joining. Nerdio Manager also adds auto-scaling for both storage types, so you only pay for the capacity you're actually using instead of over-provisioning up front.

In this section:

1. [Permissions Required to Join Azure Files Share to Domain \(Active Directory\) \(145\)](#)
2. [Create and manage configured Azure Files shares \(148\)](#)
3. [Auto-scale for Azure Files Storage Premium \(155\)](#)
4. [Auto-scale History for Azure Files Shares \(163\)](#)

5. [Create and Manage Configured Azure NetApp Files \(165\)](#)
6. [Auto-scale for Azure NetApp Files \(167\)](#)
7. [Auto-scale History for Azure NetApp Shares \(171\)](#)

Permissions Required to Join Azure Files Share to Domain (Active Directory)

This article explains the permissions required for a non-administrator, delegated domain user service account used to join an Azure Files share to an Active Directory domain. If these permissions are not correct, you receive an error during the domain join step. Errors may include, but not limited to, "Access is denied" or "A required privilege is not held by the client."

This does not apply to Entra Domain Services environments. Entra Domain Services environments only need the feature enabled and they do not need to join the domain as a specialty service account. In Nerdio Manager, be sure to select **Entra Domain Services** in the **Join to AD** drop-down list.



Note

For ease of deployment, you can use a domain administrator or temporarily elevate the delegated service account to domain administrator rights.

A domain administrator account is sufficient to join the Azure Files share to your domain. However if you are using a service account and delegating specific permissions to that account, *the "Add/Remove computer accounts" delegated permissions used for AVD session hosts are not sufficient to add Azure Files shares.*

 Note

- The domain join process for Azure Files must be executed in the context of a domain user. Nerdio Manager completes this process using the domain administrator credentials provided, or user credentials that have been delegated sufficient privileges following the steps detailed below. If you are not using domain administrator credentials, or if the domain administrator user does not receive **local** administrator privileges, Nerdio Manager's automation may not be able to complete the domain join.
- In order for Nerdio Manager to execute these commands as the specified user, a command to change the user context is required. In order for this to be successful, the specified user credentials must also be granted **local** administrator privileges on the temporary VM provisioned by Nerdio Manager to complete this process. If the specified user does not have local administrative privileges, you may receive an error message indicating *"Connecting to remote server azfilestmp-* failed with the following error message : Access is denied."* Please ensure the user account specified is granted local administrator permissions (for the azfilestmp-* VM **only**).
- Domain administrative (or delegated) privileges are a requirement for the Azure Files domain join module, Local administrative permissions are only required in order for Nerdio Manager to execute the domain join process automatically.

Azure Files joins the domain as a delegated service principal user object. In order to join the Azure Files storage account to the domain, the provided service account requires permissions on the target Organizational Unit (OU) that allows creating and writing new user objects. In addition, the service account also requires permission to set the Azure Files sign in account as delegated service. By default, this privilege is only provided to AD domain administrator users.

Delegate Permission to Create User Objects

The following procedure describes how to delegate permission to create and write user objects using Active Directory Users & Computers (ADUC, or dsa.msc).

To delegate permission to create user objects:

1. Locate the OU where Azure Files are to be joined.
2. Right-click the OU and select **Delegate Control**.
3. Add the Service User Account to be used for joining Azure Files to the domain.
4. Delegate permissions to **Create, delete, and manage user accounts**.
5. Select **Finish** to apply the changes.

Delegate Permission to Create Delegated Users

The following procedure describes how to allow the service user account used for joining Azure Files to the domain to mark the new object for Azure Files as a delegated service. This requires modifying the Default Domain Controllers group policy object in Group Policy Management (gpmc.msc).

To delete permission to create delegated users:

1. Right-click the Default Domain Controller's Policy and select **Edit**.
2. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
3. Locate the **Enable computer and user accounts to be trusted for delegation** policy.
4. Add to the policy the service user account name that is used to join Azure Files to the domain.
5. Close the editor.
6. Run **gpupdate /force** on all domain controllers.



Note

The policy change may take several minutes to apply after gpupdate completes.

Add Service Account in Nerdio Manager

You must provide the service account under AD Profiles in Nerdio Manager. See [Entra ID Join Feature](#) for details.

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 **Cloud Desktops > 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

Port	Protocol	Purpose
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)
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 **Cloud Desktops > 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.
 - **Performance:** From the drop-down list, select the performance tier for the file share.



Note

Premium storage accounts are backed by solid state drives and offer consistent, low-latency performance. They can only be used with Azure virtual machine disks, and are best for I/O-intensive applications, such as databases. Additionally, virtual machines that use premium storage for all disks qualify for a 99.9% SLA, even when running outside of an availability set. This setting can't be changed after the storage account is created.



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.
4. Enter the following information in the **Storage account configuration** section:
- **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.

- **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.
- **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.

- **Enable SMB Multichannel:** Select to enable.

 Note

Azure Files SMB Multichannel enables clients to use multiple network connections that provide increased performance. Increased performance is achieved through bandwidth aggregation over multiple NICs and utilizing Receive Side Scaling (RSS) support for NICs to distribute the IO load across multiple CPUs.

5. Enter the following information in the **File share configuration** section:
 - **Permissions (SMB Share Contributors):** Specify users/groups that have Storage File Data SMB Share Contributor role on 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.

 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.

- **Assign NTFS file-level permissions:** Select this option to have Nerdio Manager assign NTFS file-level permissions to newly created file shares.

 Note

- 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.

 Note

This is recommended for shares containing FSLogix profiles.

6. **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.

7. **Apply tags:** Optionally, type the **Name** and **Value** of the Azure tag to apply to the Azure Files share.
8. Select **OK** to save the configuration.

 Note

You may specify multiple tags. See this Microsoft [article](#) for details about using tags to organize your Azure resources.

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 **Cloud Desktops > 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 storage account:** Allows you to enable Entra ID host support. See [Enable Entra ID Joined Host Support \(154\)](#) for details.
 - **Auto-scale:** See [Auto-scale for Azure Files Storage Premium \(155\)](#) for more information.
 - **File handles:** Unlock files/Close open file handles.
 - **Force collect FSLogix profiles:** This will force a collection of FSLogix data on all the linked file shares
 - **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.

To bulk collect FSLogix data:

Nerdio Manager allows you to select multiple file shares that enables you to collect FSLogix data in bulk and on demand.

1. Navigate to **Cloud Desktops > Storage > Azure Files**.
2. Select the file shares that you want to collect FSLogix data for.
3. From the **Bulk actions** menu, select **Force collect FSLogix profiles for selected File Shares (x)**.

 Note

The **(x)** denotes the number of Azure Files shares the bulk action is applied to. In the example, 4 Azure Files shares have been selected.

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 \(165\)](#)

Auto-scale for Azure Files Storage Premium

Azure Files premium storage supports two generations of file shares, each billed — and auto-scaled — differently:

- **Provisioned V1:** billed by provisioned share size only, regardless of used capacity. Share sizes range from 100 GiB to 102,400 GiB. IO and network bandwidth limits scale automatically with the provisioned size, but are not separately configurable.
- **Provisioned V2:** billed by three independently provisioned values — share size, IOPS, and throughput. Share sizes range from 32 GiB to 262,144 GiB, provisioned IOPS from 3,000 to 102,400, and provisioned throughput from 100 to 10,340 MiB/s. Billing rates for all three vary by region and other parameters — see [Azure Files Pricing](#) for details.

When enabled, storage auto-scale grows the provisioned values in response to anticipated usage demand or increased storage latency. It also decreases them to reduce costs when the extra performance is no longer needed (not more than once every 24 hours per value).

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.

 Note

Auto-scale is disabled by default on a newly linked share. There is no conversion between Provisioned V1 and Provisioned V2 — the generation is fixed when the share is created, and a share is always one or the other.

You must configure these auto-scale parameters:

- Provisioned Size (Quota), IOPS and Throughput (*the values scaled depend on whether the share is Provisioned V1 or Provisioned V2 — see below*)

- Scheduled Data Increase (Optional)
- Scaling Logic

To configure and manage auto-scale for Azure Files premium:

1. Navigate to **Cloud Desktops > 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. Refer to the table that matches your share's generation (Provisioned V1 or Provisioned V2), and enter the **Provisioned Size (Quota)**, **IOPS** and **Throughput** settings listed.

Provisioned V1

UI Element	Type	Description
Quota unit	Drop-down list	Select the unit used for Minimum size and Maximum size : Relative (%) , a percentage of currently used capacity, or Absolute (GiB) , a fixed value in GiB.
Minimum size	Text field	The smallest size auto-scale will maintain, entered in GiB or % above used capacity. The minimum is 100 GiB, and cannot be set smaller than the share's current used capacity. This value defines the buffer of free space auto-scale always keeps available as used capacity grows.
Maximum size	Text field	The largest size auto-scale will grow the share to, entered in GiB or % above used capacity, up to a ceiling entered in the Less than field. Auto-scale increases the share only up to this maximum, to prevent uncontrolled growth.

UI Element	Type	Description
Performance	Read-only display	Shows the minimum and maximum performance characteristics that result from the configured size range. These values are calculated by Azure from the provisioned size and cannot be configured directly: • IO/S: baseline IOPS, calculated as $3,000 + 1$ per provisioned GiB, up to a maximum baseline rate of 100,000 IO/s. • Burst IO/S: the greater of 10,000 IO/s or 3x the baseline IO/s rate. Unused baseline IO accumulates as burst credits (up to a limit) that are drawn down when demand exceeds the baseline rate, up to a maximum burst rate of 100,000 IO/s. • Egress Rate: allowed network egress per second, calculated as $60 + (\text{share quota} \times 0.06 \text{ MiByte/s})$. • Ingress Rate: allowed network ingress per second, calculated as $40 + (\text{share quota} \times 0.04 \text{ MiByte/s})$.

Provisioned V2



Note

Billing rates for provisioned size, IOPS, and throughput vary by region and other parameters. See [Azure Files Pricing](#) for details.

UI Element	Type	Description
Quota unit	Drop-down list	Select the unit used for Minimum size and Maximum size : Relative (%) , a percentage of currently used capacity, or Absolute (GiB) , a fixed value in GiB.
Minimum size	Text field	The smallest size auto-scale will maintain, entered in GiB or % above used capacity. The minimum is 32 GiB, and cannot be set smaller than the share's current used capacity.
Maximum size	Text field	The largest size auto-scale will grow the share to, entered in GiB or % above used capacity, up to a ceiling entered in the Less than field (maximum 262,144 GiB). Auto-scale increases the share only up to this maximum, to prevent uncontrolled growth.

UI Element	Type	Description
Provisioned IOPS	Text fields (from / to)	The range auto-scale keeps provisioned IOPS within. Provisioned V2 caps IOPS at 5x the value Microsoft recommends for the share's current size, and never above the tier's absolute maximum (102,400 IOPS on this tier). The cap rises as the share grows — for example, at 32 GiB the ceiling is 15,160 IOPS, rising to 102,400 IOPS at the configured maximum of 262,144 GiB. Auto-scale does not grow the share purely to reach a higher IOPS cap; raising the Minimum size is what lifts the cap sooner.
Provisioned throughput (MiB/s)	Text fields (from / to)	The range auto-scale keeps provisioned throughput within. Provisioned V2 caps throughput at 5x the value Microsoft recommends for the share's current size, and never above the tier's absolute maximum (10,340 MiB/s on this tier). The cap rises as the share grows — for example, at 32 GiB the ceiling is 520 MiB/s, rising to 10,340 MiB/s at the configured maximum of 262,144 GiB. Auto-scale does not grow the share purely to reach a higher throughput cap; raising the Minimum size is what lifts the cap sooner.

- Optionally, toggle **Scheduled Quota Increase** (Provisioned V1) or **Scheduled Performance Increase** (Provisioned V2) to **On**. This commits to a temporary increase during a recurring window — for example, if you have days with predictable peak demand. While the schedule is active, the scheduled values are held and latency-based scaling rules do not apply to them. Refer to the table that matches your share's generation, and enter the settings listed.

Provisioned V1



Note

Provisioned size (quota) can be decreased only 24 hours after the last quota increase. The quota is increased at the beginning of the scheduled period and decreased to the minimum size only at the end of it.

UI Element	Type	Description
Days	Drop-down list	Select the range of days the schedule applies to.
Hours	Time range and drop-down list	Set the start and end time of the scheduled window, and select the time zone it applies in.
Set provisioned size (quota) to	Text field	The quota, above current used capacity, that the share is set to for the duration of the scheduled window.

Provisioned V2

Note

Provisioned IOPS and throughput can each be decreased only 24 hours after their own last increase. Both are increased at the beginning of the scheduled period and decreased to their minimum values only at the end of it.

UI Element	Type	Description
Days	Drop-down list	Select the range of days the schedule applies to.
Hours	Time range and drop-down list	Set the start and end time of the scheduled window, and select the time zone it applies in.
Set provisioned IOPS to	Text field	The provisioned IOPS value the share is held at for the duration of the scheduled window.
Set provisioned throughput (MiB/s) to	Text field	The provisioned throughput value the share is held at for the duration of the scheduled window.

- These conditions determine when auto-scale increases or decreases the provisioned values: any rule proposing an increase causes an increase, and a decrease is applied when a rule proposes one. Refer to the table that matches your share's generation, and enter the **Scaling Logic** settings listed.

Provisioned V1

Note

Provisioned size (quota) can be decreased only 24 hours after the last quota increase.

Provisioned V1 supports up to two rules, both targeting size (quota): one for scale-out, one for scale-in.

UI Element	Type	Description
Select auto-scale trigger	Drop-down list	The latency metric that drives scaling: Success Server Latency (avg) (default) or Success Server Latency (max) — the average or maximum time Azure Storage takes to process a successful request.
Increase quota (scale out) by	Text field (%)	The step size to increase the quota by (in the unit set under Quota unit) each time the scale-out condition below is met. While the latency threshold is exceeded, the system keeps scaling out until it either reaches the configured maximum size or the latency drops back under the threshold.
if Success Server Latency exceeds	Text field (ms)	The latency threshold, in milliseconds, that triggers a scale-out.
for ... Minutes (scale-out)	Drop-down list	The measurement window the scale-out latency threshold must be sustained for: 5, 15, 30, or 60 minutes.
Decrease quota (scale in) by	Text field (%)	The step size to decrease the quota by each time the scale-in condition below is met.
if Success Server Latency drops below	Text field (ms)	The latency threshold, in milliseconds, that triggers a scale-in.
for ... Minutes (scale-in)	Drop-down list	The measurement window the scale-in latency threshold must be sustained for: 5, 15, 30, or 60 minutes.

Provisioned V2

Note

Provisioned IOPS and throughput can each be decreased only 24 hours after their own last increase.

Provisioned V2 supports up to four rules — a scale-out and a scale-in rule for each of Provisioned IOPS and Provisioned throughput. Select **+** to add a rule and choose which value it targets.

UI Element	Type	Description
Type	Drop-down list	• Provisioned IOPS: this rule scales provisioned IOPS. • Provisioned throughput: this rule scales provisioned throughput (MiB/s). Each rule targets one value in one direction. Up to four rules can exist at once: scale-out and scale-in, for each of IOPS and throughput.
Select auto-scale trigger	Drop-down list	The latency metric that drives scaling — the average or maximum time Azure Storage takes to process a successful request. The options available depend on the Type selected above: • Type: Provisioned IOPS — both Success Server Latency (avg) (default) and Success Server Latency (max) are available. • Type: Provisioned throughput — only Success Server Latency (max) is available.
Increase provisioned IOPS / throughput (scale out) by	Text field (IOPS or MiB/s)	The step size to increase the value selected under Type by, each time the scale-out condition below is met. The increase is bounded by the value's cap (see Provisioned IOPS / Provisioned throughput in the previous step).
if Success Server Latency exceeds	Text field (ms)	The latency threshold, in milliseconds, that triggers a scale-out.
for ... Minutes (scale-out)	Drop-down list	The measurement window the scale-out latency threshold must be sustained for: 5, 15, 30, or 60 minutes.
Decrease provisioned IOPS / throughput (scale in) by	Text field (IOPS or MiB/s)	The step size to decrease the value selected under Type by, each time the scale-in condition below is met.

UI Element	Type	Description
if Success Server Latency drops below	Text field (ms)	The latency threshold, in milliseconds, that triggers a scale-in.
for ... Minutes (scale-in)	Drop-down list	The measurement window the scale-in latency threshold must be sustained for: 5, 15, 30, or 60 minutes.

- 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 \(167\)](#)

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.

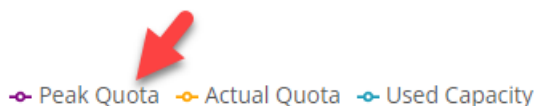
- **Time Range:** At the top of the window, select the desired time range to display.
- **Show:** At the top of the window, select the desired graph(s) to display.
- **Savings:** At the top of the window, you can view auto-scale savings.
- **Zoom In:** For the **Quota (GiB)** graph only, click and drag 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 **Cloud Desktops > 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 \(171\)](#)

Create and Manage Configured Azure NetApp Files

Note

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.

Link the Azure Subscription and Resource Group to Nerdio Manager

You must link the Azure subscription and resource group where the Azure NetApp Files resides to Nerdio Manager before you can proceed to the next steps.

To link the Azure subscription to resource group to Nerdio Manager:

1. Navigate to **System > Settings > Azure**.
2. Expand **Azure Subscriptions**.
3. Select either **Link using currently logged in user** or **Link using app credentials** to link the Azure subscription.
4. Expand **Linked Resource Groups**.
5. Select **Link** to link the resource group.

Link to an Existing Azure NetApp Files Share

You can link to an existing Azure NetApp Files share.

To link to an existing Azure NetApp Files share:

1. Navigate to **Cloud Desktops > 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

You can create an Azure files and/or storage account.

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 **Cloud Desktops > 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 \(148\)](#)

Auto-scale for Azure NetApp Files

 Note

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 **Cloud Desktops > 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 ScalingOn** 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 ScalingOn** 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 \(155\)](#)

Auto-scale History for Azure NetApp Shares

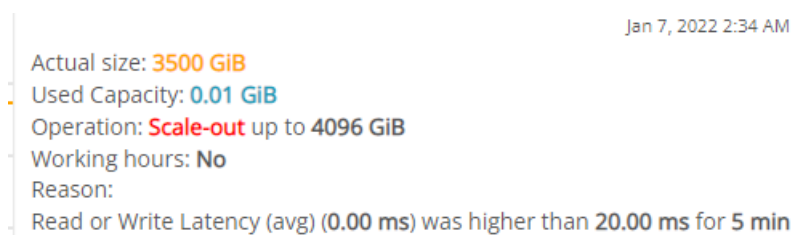
Note

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.

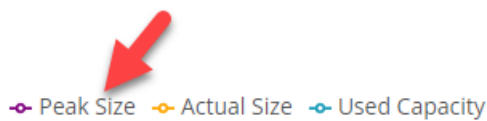
The following are important auto-scale history features.

- **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:

1. Navigate to **Cloud Desktops > Storage > Azure NetApp 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.
 - **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 \(163\)](#)

Step #5: FSLogix and User Profile Management

With storage in place, the next step is to configure **FSLogix**, the profile management solution that lets user settings, data, and installed applications follow

users between session hosts. This section covers setting up FSLogix, tuning its configuration per host pool, and managing which applications are available to users.

In this section:

1. [FSLogix and User Profile Management \(173\)](#)
2. [FSLogix settings and configuration \(174\)](#)
3. [FSLogix per-host pool customization \(178\)](#)
4. [Manage Installed Applications on Host Pools \(182\)](#)

FSLogix and User Profile Management

FSLogix is a user profile container technology that allows users to switch virtual desktop session hosts 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 legacy RDS User Profile Disks (UPDs).

FSLogix is integrated with AVD, and provides a seamless, on-demand seamless 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 (i.e. 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. You can create multiple FSLogix configuration profiles, and apply them on a per-host pool basis. This means you can have different FSLogix configurations where, for example, the storage locations are different, or where you have different registry parameters set at the per-host pool level.

**Note**

- The most common FSLogix Profile storage solution, and the one generally recommended for new deployments/Profiles, is Azure Files Storage. See [Create and Manage Configured Azure Files Shares \(148\)](#) for detailed configuration instructions.
- If you're unsure which storage solution to choose for your environment, see [Which FSLogix Profile storage option should I choose?](#)

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. This ensures 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 \(174\)](#)

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 **Cloud Desktops > Azure Virtual Desktop > Host Pool Profiles**.
2. From the bottom right-hand side, select **New profile**, and from the menu options, select **FSLogix**

3. In the **FSLogix Profiles storage** area, select **Add**.
4. 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.

- **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.
- **Exclude domain account from FSLogix:** Select this option to prevent domain account profiles from being created in the FSLogix storage location, and then enter the domain details in the box below.

 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 edit the FSLogix App Service Registry settings.
- **Manage Log settings:** Select this option to manage log settings.
- **FSLogix Profiles path (VHDLocation):** 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 **Edit mode** drop-down list, select whether you want to work with **All settings** or **Advanced**.
 - For **All settings**:
 - In the **Configuration** column, enter 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**. For example: "**ProfileType**"=dword:00000003.
 - You can add string values in the format: "**ValueName**":"**ValueData**". For example: "**VolumeType**":"vhdx".
- **Configure Office Container to redirect Microsoft Officer 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:** From the **Edit mode** drop-down list, select whether you want to work with **All settings** or **Advanced**, and then configure the settings as required.
- **Redirections:** Toggle this option on 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.

5. 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 **System > Settings > Integrations**.
2. In the **FSLogix Profiles storage** area, add, change, and remove the profiles as needed.

 Note

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**.

 Note

- 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 \(173\)](#)

[FSLogix Per-Host Pool Customization \(178\)](#)

[Which FSLogix Profile storage option should I choose?](#)

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 \(64\)](#).

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. Select the more options  menu, and then select **Settings**.
3. From the menu options on the left-hand side, select **FSLogix**.
4. Enter the following information:
 - **Enable FSLogix profiles:** Select the toggle to enable FSLogix profiles.

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.

- From the drop-down list, select an existing profile name. Alternatively, select **Custom** to create a custom profile for this host pool.

Note

If you select an existing profile then this will automatically complete the configuration with the detail in the selected profile, which cannot be edited. If you select **Custom** you can configure the profile as required.

- **Version** From the drop-down list, select the FSLogix version.
- **Configure session hosts registry for Entra ID joined storage:**
- **Exclude the local admin accounts from FSLogix:**
- **Exclude domain accounts from FSLogix:**
- FSLogix profiles path (VHDLocation).
- Configure Office Container to redirect Microsoft Office user data (ODFC):
 - FSLogix Office Container path (VHDLocation):
- **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 scenario).

 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.

- **Manage App Service settings:** Select this option to edit the FSLogix app service registry settings.
- **Manage Log settings:** Select this option to manage log registry settings.
- **FSLogix registry options:** From the **Edit mode** drop-down list, select whether you want to work with **All settings** or **Advanced**.
 - For **All settings**:
 - From the tabs, select the component you want to configure. Select from **Profile Settings**, **ODFC Settings**, **Cloud Cache Settings**, **App Service Settings**, or **Log Settings**.

- In the **Configuration** column, type the setting's value. For example, to configure profile settings, select the **Profile Settings** area, select the box in the **Configuration** column, and enter the setting.
- Select **Clear tab configuration values** to set all values for that particular component as **Not configured**.
- Select **Clear all configuration values** to set all the settings to **Not configured**.
 - Optionally, in the **Search settings by name** box, you can filter the settings by entering the name or part of the name of the setting.
- 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").*
- **Redirections**: If you want to include redirections in the global profile for re-use across customers select the toggle to enable this feature.

Note

For more details, see [Types of containers](#).

- **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**: To send messages to active users, select the toggle to enable this feature and enter the following details:
 - **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**: To apply the changes at a selected time, select the toggle to enable this feature and enter the following details:
 - **Name**: Enter a name for the schedule.

- **Description:** Enter a description for the schedule.
- **Start Date:** Select the **Start Date** box and from the calendar, select the desired start date..
- **Time Zone:** From the drop-down list, select the time zone for the Start time.
- **Start Time:** From the drop-down lists for hours and minutes, 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.
5. Once you have entered all the desired information, select **Save** or **Save & close**.

Related topics

[Host Pools \(64\)](#)

<https://www.youtube.com/watch?v=HJMLL3ZthPs>

Manage Installed Applications on Host Pools

Nerdio Manager allows you to leverage FSLogix App Masking technology to automatically discover applications installed on a host pool and configure rules to determine which users can access which applications. User access can be controlled at the individual application level and can be assigned by user or security group. Multiple applications can be grouped together for consolidated access management. Simply install all the required applications on the desktop image, update the session hosts, and define which users can access which applications.

 Note

FSLogix App Masking is currently not supported in AAD joined host pool scenarios.

 Note

This process does not work by simply hiding shortcuts. It actually hides all the components of the application. For example, if you create a rule to hide Chrome from all users:

- The Chrome folder in Program Files appears to the user to be empty. In fact, the folder is not empty, it is just hidden from the user.
- Chrome is unpinned from the taskbar, if necessary.
- The Chrome desktop shortcut is removed, if necessary.
- The user does not find Chrome when performing a Cortana search.

The following steps must be performed in order to manage the installed apps:

- **Discover and edit installed applications:** The discovery is automatically performed whenever a host pool is created or re-imaged. In addition, it is also runs every few days in order to find applications that may have been added (not through a re-image process). Alternatively, the discovery can be run manually.
- **Create rule sets:** Create rule sets to determine which users have access to which applications.
- **Apply the rule sets to the session hosts VMs:** Apply the selected rule sets to all the session host VMs. You can wait to perform this when a session host is created or re-imaged. Alternatively, you can manually apply the selected rule sets immediately.

These steps are discussed in detail below.

Discover and Edit Installed Applications

The first step to managing the installed applications is to discover the applications that are installed. In addition, Nerdio Manager allows you to edit and manually add applications.

To discover and edit the installed applications:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications> Installed apps**.
3. Note the date and time the discovery was last performed.

Note

If the host pool was created recently, you may not see any discovered applications because a discovery has not yet been performed yet. You may need to wait up to 48 hours or initiate a manual discovery.

4. If desired, select **(nn apps)** to see a list of discovered applications and additional details.
5. If desired, select **Discover apps** to perform a manual discovery.
 - Enter the following information:
 - **Session Host VM**: From the drop-down list, select the session host VM you want to use to perform the discovery.
 - Select **Advanced** to perform any of the following:
 - Select  to remove a discovered application.
 - Edit the name or installation directory information for any discovered application, if desired.
 - Select  to add an application and its installation directory. The discovery process looks for all the components of this application in this directory and automatically detects them.
 - Once you have entered all the desired information, select **Run now**.
 - Watch the discovery process's progress in the tasks pane. Be sure to wait for the task to finish before continuing.

 Note

If the session host VM is powered off, the system powers on the VM to perform the discovery.

Create Rule Sets

The next step to managing the installed applications is to create rule sets. In essence, you determine which users have access to which applications.

To create rule sets:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications> Installed apps**.
3. Select **Add rule set**.
4. Enter the following information:
 - **Rule Set Name:** Type the name of the rule set.
 - **Enabled:** Select this option to enable the rule set.

 Note

Only rule sets that are enabled are applied to hosts.

- **Applications:** From the drop-down list, select the discovered applications to add to the rule set.
 - If desired, expand the application to see its details.
 - Edit, add, or delete the application's components, as desired.
- **Rule Type: App Masking:** This allows you to manage access of installed components.
- **Rule Type: Redirection:** This enables you to dynamically redirect a folder, file, registry key, or value to an alternative based on the user or group. For example, as shown above, you can have an app use a different license file for the sales team.
- **Rule Type: App Container:** This enables you to dynamically redirect a folder to another attached disk. For example, as shown above, redirect to another drive that contains the licenses for the sales team.

- **Apply to all users:** When this option is selected (default), the applications are available only to users you specify in the **Exclude users and groups** field. The applications are hidden and unavailable for any other users.

 Note

- Unselect this option if you need to make the applications available for all users.
- If you still need to restrict access for some users or groups, include those in the **Apply only the following users and groups** field.

Note that the **Apply only the following users and groups** field becomes available only when the **Apply to all users** option is disabled.

- **Exclude local administrators:** Select this option to not apply this rule to the local administrators group.
 - **Exclude users and groups:** Select the users to exclude from the allowlist or the blocklist.
5. Select **Save & apply** to save the rule and apply it immediately to all session host VMs. Select **Save & close** to save the rule.

 Note

When you select **Save & close**, the rule is applied when a session hosts are created or re-imaged. Alternatively, you can manually apply the rule later on when desired.

Manage and Apply Rule Sets

Nerdio Manager allows you to manage rule sets. This includes applying rule sets, deleting, editing, etc.

To manage rule sets:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications> Installed apps**.
3. You may select multiple rules and then **Select bulk action** to perform a bulk action on the selected rules.

4. From the action menu next to each rule set, you can:
 - Select **Edit** to edit the rule set.
 - Select **Apply to hosts** to immediately apply the rule set to all session hosts. (see below)
 - Select **Disable** to disable the rule set.
 - Select **Delete** to delete the rule set.
 - Select **Assign** to change the rule set assignments.
5. In addition, you can:
 - Select **Discover apps** to immediately start the applications discovery process. (see above)
 - Select **Add rule set** to add a new rule set. (see above)
 - Select **Apply all rule sets** to immediately apply all the rule sets to all the session hosts. (see below)

To apply rule sets:

1. Select **Apply to hosts** (for a single rule or selected rules) or **Apply all rule sets** (for all rules).
2. Enter the following information:
 - **How to apply:** From the drop-down list, select how the rule set should be applied.
 - **Clear all existing FSLogix rule sets on hosts:** Select this option to clear all the FSLogix rule sets on the hosts before applying this rule set.
 - **Clear only Nerdio Manager created rule sets on hosts:** Select this option to clear all the rule sets that were created by Nerdio Manager on the hosts before applying this rule set.
 - **Do not clear any rule sets, overwrite rule sets being applied only:** Select this option to leave all the existing rule sets alone and only overwrite the rule set that is being applied.
 - **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.

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

The rule set application process starts.

Export Rule Sets

Nerdio Manager allows you to export rule sets to either a JSON file or a host pool.

To export rule sets:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications> Installed apps**.
3. Select the rule set(s) you wish to export.
4. From **Select bulk action** action menu, select **Export rule sets**.
5. Enter the following information:
 - **Export to:** From the drop-down list, select the export destination.

Note

When exporting to a JSON file, the file is downloaded to the browser's default download folder.

- **Destination host pool:** When exporting to a host pool, from the drop-down list, select the host pool.
6. Once you have entered all the desired information, select **OK**.

The rule set export process starts.

Import Rule Sets

Nerdio Manager allows you to import rule sets that were previously exported in a JSON file or from a host pool.

To import rule sets:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications> Installed apps**.
3. From the **Add rule set** action menu, select **Import rule sets**.
4. Enter the following information:

- **Import from:** From the drop-down list, select the import location.
- **Host pool:** When importing from a host pool, from the drop-down list, select the host pool.
- **JSON file:** When importing from a JSON file, select the file.
- **Activate imported rule sets:** Select this option to activate the imported rule sets after they are imported.

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

The rule set import process starts.

Step #6: MSIX App Attach

The next step is to configure **MSIX App Attach**, Nerdio Manager's method for delivering applications to session hosts without installing them directly on the image.

An MSIX App Attach image is an expanded container - a VHD, VHDX, or CIM file - holding one or more extracted MSIX packages. Nerdio Manager mounts these images to session hosts in the host pool, making the packaged applications available to users as soon as they sign in.

In this section:

1. [Manage App Attach images and packages \(189\)](#)
2. [Manage App Attach Assignments \(196\)](#)
3. [Configure Azure Files Permissions for App Attach \(199\)](#)

Manage App Attach images and packages

Nerdio Manager allows you to manage App Attach images and packages.

Sample Workflow

The following is a sample workflow:

- Upload the App Attach image to the Nerdio Manager-managed image library. See [Upload an App Attach image file \(191\)](#) and [Upload an MSIX package file \(192\)](#).
- Add the App Attach images in the Nerdio Manager-managed image library as App Attach packages in Azure. See [Use the App Attach package wizard \(193\)](#).

 Note

The App Attach package wizard allows you to assign users and groups in a host pools to the App Attach package.

- You can manage image versions, as needed. See [Upload a new version of an app \(195\)](#) and [Manage Nerdio App Attach image versions \(196\)](#).
- You can manage assignments, as needed. See [Manage App Attach Assignments \(196\)](#).

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 App Attach image file

You can upload an VHD/VHDX/CIM image to the Nerdio Manager-managed image library.

To upload an image:

1. Navigate to **Applications > Catalog > App Attach**.
2. Select the **Nerdio App Attach Images** area.
3. Select **Upload image**.
4. Enter the following information:
 - **Friendly name:** Type the name that you want to appear on the images list.
 - **Description:** Type a description.
 - **Version:** Type the version number of the image that you are uploading. This must be unique.
 - **Storage locations:** From the drop-down list, select the linked app storage location(s) in the AD-integrated Azure Files share.



Note

- App Attach does not support Entra Domain Services. This needs to be Active Directory Domain Services (ADDS).
- For App Attach working in Entra ID, you should enable **Entra ID Host support**. Navigate to **Storage > Azure Files > Manage storage account**.

- **Image File(s):** Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from MSIX installer or upload file(s) of the App-V package.
- **Certificate (.cer) file(s):** Select the certificate file(s).

 Note

A certificate that was used to create the package must be installed on all session hosts VMs. If you used a self-signed certificate to create the 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

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

The image is uploaded to Nerdio Manager.

Upload an MSIX package file

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. The VHD image is added to the Nerdio Manager-managed image library.

To upload an MSIX package file:

1. Navigate to **Applications > Catalog > App Attach**.
2. Select the **Nerdio App Attach Images** area.
3. Select **Upload MSIX apps(s)**.
4. Enter the following information:
 - **Image name:** Type the image name.
 - **Storage locations:** From the drop-down list, select the storage locations where the App Attach application are stored. .

 Note

- Storage location should be in the same Azure region as the session host VMs that access the app.
- In **Premium** and **Core** editions only, the first selected location is considered to be primary. The primary location contains all versions of the application.

- **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.

5. 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.

Use the App Attach package wizard

The App Attach package wizard adds the selected App Attach images in the Nerdio Manager-managed image library as App Attach packages in Azure. In addition, it allows you to assign the packages to all the desired users and groups in the specified host pools.

To use the App Attach package wizard:

1. Navigate to **Applications > Catalog > App Attach**.
2. Select the **App Attach Packages** area.
3. Select **+ Add App Attach package**.
4. Alternatively, from the **Nerdio App Attach Images** area:
 - Locate the image you wish to work with.
 - From the action menu, select **Package wizard**.

5. Enter the information in the App attach wizard.
6. In the **Image** area, enter the following information:
 - **Image source:** From the drop-down list, select the image source.
 - **App Attach Image:** From the drop-down list, select the application image.
 - **Image Version:** From the drop-down list, select the version of the application image.
 - **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

- The 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.
- The temporary host pool is also used to expand the image and test if the image is valid.

7. In the **Package** area, 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.
8. In the **Assignments** area, 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).
9. In the **Summary** area, review the selections.
 10. 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 **Tasks** window.

Upload a new version of an app

Nerdio Manager allows you to have multiple versions of an app. Therefore, you can upload new versions of an app as desired.

To upload a new version of an app:

1. Navigate to **Applications > Catalog > App Attach**.
2. Select the **Nerdio App Attach Images** area.
3. Locate the image you want to work with.
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.
 - **Storage locations:** Select the storage locations where the App Attach application is to be stored.

Note

Storage location should be in the same Azure region as the session host VMs that are accessing the app.

- **Image file(s):** From the drop-down list, select the application image.
- **Certificate (.cer) File(s):** Optionally, select the certificate file(s).

 Note

A certificate that was used to create the package must be installed on all session hosts VMs. If you used a self-signed certificate to create the 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**.

Manage Nerdio App Attach image versions

Nerdio Manager allows you to manage image versions. This includes uploading a new image, changing its storage location, or updating the host pools with the desired version.

To manage image versions:

1. Navigate **Applications > Catalog > App Attach**.
2. Select the **Nerdio App Attach Images** area.
3. Locate the image you want to work with.
4. Select the **Image versions** icon. 
5. Locate the image version you wish to set as the default.
6. Perform any of the following on the image version:
 - Select the **Update host pools** icon  to update the assigned host pools with the selected version.
 - From the action menu, select **Change storage locations**, to change the image's storage location.
7. Alternatively, select **+ Upload new version** to upload a new version.

Related Topics

[Manage App Attach Assignments \(196\)](#)

Manage App Attach Assignments

Nerdio Manager allows you to assign users and groups in host pools to App Attach packages. You must first upload an App Attach image and add an

App Attach package before you can perform the assignments. See [Manage App Attach images and packages \(189\)](#) for details.

**Note**

These assignments can be performed by using the App Attach package wizard. See [Manage App Attach images and packages \(189\)](#) for details.

Add an MSIX App Attach package to a host pool

You can assign an MSIX App Attach package to a host pool.

**Warning**

MSIX App Attach is deprecated. The feature does not receive any further updates from Microsoft. It is recommended that all new packages be created as App Attach.

To add an MSIX App Attach package to a host pool:

1. Locate the host pool you wish to assign the app to.
2. From the more actions menu  icon, select **Applications > Catalog > App Attach**.
3. When the **App Attach** window is displayed, from the more actions menu  icon select **Add MSIX App Attach package**.
4. Enter the following information:
 - **Image Source:** From the drop-down list, select the location of the image that contains MSIX packages.

 Note

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

Assign an App Attach package to users and groups in host pools

You can assign the package to users and groups in host pools.

To assign an App Attach package to users and groups:

1. Navigate to **Applications > Catalog > App Attach**.
2. Select the **App Attach Packages** area.
3. Locate the App Attach package you want to work with.
4. Select the **Assignments** icon. 
5. Enter the following information:
 - **Users and groups:** From the drop-down list, select the users and groups to assign the package to.

 Note

You must specify users and/or groups.

- **Host pools:** From the drop-down list, select the host pools to assign the package to.

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

Assign App Attach packages to a host pool

You can assign App Attach packages 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 more actions menu  icon, select **Applications > Catalog > App Attach**.
3. When the **App Attach** window is displayed, select **Assign App Attach packages**.
4. Enter the following information:
 - **App Attach Packages:** From the drop-down list, select the App Attach package(s).
5. Once you have entered all the desired information, select **OK**.

Configure Azure Files Permissions for App Attach

Nerdio Manager leverages Azure Files share technology to store App Attach packages and associated metadata. You can use an existing Azure Files share or create a new one with Nerdio Manager.



Note

The Azure Files share must be AD-integrated to be used as an App Attach storage location in Nerdio Manager.

Once you've created an Azure Files share and joined it to your AD domain, you must configure security settings on the share to allow session hosts and users to read the contents of the App Attach packages. With Azure Files, the security settings are configured in the following places:

Azure Files Access

NTFS Permissions

In these places, both the session host VM computer and user who uses the application must have at least **Reader** access. By default, the NTFS permissions on newly created Azure Files shares already have the necessary configuration. However, Azure Files share Access Control still needs to be configured.

To grant session host VMs access to Azure Files shares:

1. In Active Directory, create a new Global Security group in an OU that is being synched to Entra ID with ADConnect.
2. Add **Domain Computers** and **Domain Users** to the new group.
3. In Azure portal, find your Azure Files share and navigate to **Access Control**.
4. Add the new security group with Storage File Data SMB Share Reader role.

Note

You may need to wait for the next sync cycle for new groups to be available in Entra ID.

Note

The end result is read-only access to the Azure Files share by all domain users and computers. Feel free to customize the above procedure to suite your organization's security policies.

Step #7: Role-based Access Control (RBAC)

The final step is to configure **role-based access control (RBAC)**, so the right people on your team have the right level of access to Nerdio Manager - from full administrators down to help-desk staff who only need to perform specific tasks.

In this section:

1. [Role-based access control \(RBAC\) in Nerdio Manager \(201\)](#)
2. [Role-based access control \(RBAC\): Custom roles \(204\)](#)
3. [Role-based Access Control \(RBAC\): Multiple Group Assignments \(207\)](#)

Role-based access control (RBAC) in Nerdio Manager

Note

There is an Entra ID limitation that the owner role on a enterprise app is only automatically assigned to a direct user and cannot be assigned to a group using Nerdio Manager. Therefore, admins in Nerdio Manager must be directly assigned so that Nerdio Manager adds the owner role automatically.

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 \(204\)](#).

Companion Video

<https://fast.wistia.net/embed/iframe/e1e4p9ff5r?seo=false&videoFoam=true>

Users and roles management

Nerdio Manager enables you to view the configured role based access role assignments.

To show RBAC role assignments:

- Navigate to **System > RBAC > Assignments**. The list of users and their RBAC role assignments are displayed.



Note

- 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

You can add users to Roles/Workspaces.

To add users to Roles/Workspaces:

1. Navigate to **System > RBAC > Assignments**.
2. Do the following:

Select **New Assignment**.

3. In the **Add Role** dialog box, 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**.

 Note

- 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 role

You can change a user's role or the Workspaces the user has access to.

To edit a user:

1. Navigate to **System > RBAC > Assignments**.
2. Do the following:

Locate the user you wish to edit, and select the edit  icon.

3. 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 **System > RBAC > Assignments**.

- Do the following:

Locate the user you wish to remove access from, and from the more actions  menu, select **Remove access**.

2. 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 role definitions 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 manage mode.

To create a custom role definition:

1. Navigate to **System > RBAC > Definitions**.

2. Select **New Definition**.

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.

Table 1.

Module	Modes
OBSERVABILITY	
Insights	• Read Only: Provides users with read-only access to the Insights dashboards. • Manage
Observability > Advisor > Modeler	• Read Only • Manage

Module	Modes
Observability > Advisor > Recommendations	• Read Only • Manage
Observability > Advisor > Rules	• Read Only • Manage
AVD & SESSIONS	
Workspaces	• Read Only • Manage • 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. • Run scripted actions: Allow users to run scripted actions within assigned host pools. • Console Connect Operator: Allows users to manage Console Connect roles.
Desktop images	• Read Only • Manage
App attach	• Read Only • Manage
Portal	• Manage
ENDPOINT MANAGEMENT	
Intune (Global Roles)	• Read Only • Manage
Intune (Read Only Roles)	• 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 • Read Approvals

Module	Modes
Intune (Manage Roles)	• Manage Devices • Manage Devices Privileged • Manage BitLocker • Manage Antivirus • Manage Device Groups • Manage User Groups • Manage Locate Device • Manage Policies • Manage Applications and App Policies • Manage Update Rings and Policies • Console Connect Operator • Manage Approvals • Manage Scripts • Manage Microsoft licenses
Intune > Windows 365	• Read Only • Manage
APP MANAGEMENT (UAM)	
UAM > Deployment policies	• Read Only • Manage
UAM > App groups	• Read Only • Manage
UAM > Unified catalog	• Read Catalog • Manage Catalog: Allow users to manage UAM catalogs and perform tasks such as importing and deploying apps. • Manage Shell App Parameters: Allow users to manage Shell App parameters.
AUTOMATION	
Scripted actions	• Read Only • Manage
Scripted sequences	• Read Only • Manage
Scripted sequences > executions	• Read Only • Manage
Task worker analytics	• Read Only • Manage
STORAGE	
Cloud desktops > Storage > Azure Files	• Read Only • Manage • 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.
Cloud desktops > Storage > Azure NetApp Files	• Read Only • Manage

Module	Modes
Cloud desktops > Storage > Log Analytics	• Read Only • Manage
OPERATIONS	
Monitoring	• Read Only
Logs	• Read Only
Migrate	• Read Only • Manage
Secure variables	• Read Only • Manage • Show Secret

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](#).

Role-based Access Control (RBAC): Multiple Group Assignments

When using one of the built-in accounts, administrative access to Nerdio Manager is controlled by individual user or group assignment to Nerdio Manager's application registered in Entra ID. As of Nerdio Manager v6.4, support for Cumulative RBAC has been introduced for custom roles. Please review this document carefully to understand the implications of this change. Details on the new and previous behavior are described below.

While it is possible for a user to be entitled to Nerdio Manager through multiple group memberships, this is not a supported configuration if using built-in accounts, or a combination of built-in accounts and custom roles. Care should be taken to ensure that users only have one assignment granting access to Nerdio Manager if using built-in accounts.

RBAC Considerations from Nerdio Manager v6.4 and later

Note

The behavior described here is default for new installations of Nerdio Manager. For existing installs, if cumulative RBAC functionality is desired, this must be enabled by the app service setting **Features:CumulativeRbac** with a value of **True**.

With the release of Nerdio Manager v6.4, the concept of cumulative RBAC has been introduced for custom roles. This new functionality allows for different permissions, which may be assigned via separate individual assignments user or group memberships, to be applied cumulatively within the Nerdio Manager console.

Where conflicts are present within the assigned roles, the higher permission assignment is applied. Ensure the permissions you assign to users and groups via custom roles meet or exceed your organization's security requirements.

Note

Multiple direct assignments are not supported. A single direct assignment may be combined with multiple **indirect (group)** assignments. This new functionality applies only to custom roles defined within the Nerdio Manager application. Built-in roles are fully excluded from this new functionality.

Core Permission Assignment Principles

The following are the core principles related to how the permission assignments apply through Entra ID and how Nerdio Manager interprets them.

- Users can be assigned directly to the application with a specific role and workspace combination, or they can be a direct member of a group that is

assigned to the application. Assignments as both a user and group member are supported

- Members of a group that is a nested member of another group, which is assigned to the Entra ID application, are not considered. This is an Entra ID limit. See this Microsoft [article](#) for details.
- Nerdio Manager's built-in default roles are arranged in order of tiers with decreasing permission. If a user is a member of groups with multiple equivalent built-in role tiers, then Entra ID only provides one of those assignments to Nerdio Manager. In general, it is provided alphabetically, so the first alphabetical group's assignments apply in most situations, but technically it can be processed in any order.

Additional Principles

- Nerdio Manager's Custom Roles provide a filtered experience at the application level. Therefore, custom roles provide the ability to assign one or more custom roles via direct assignment or group membership, and these roles are combined within the Nerdio Manager application to provide the most permissive set of permissions.
- A direct user assignment is considered the highest priority. Therefore, any user directly assigned to Nerdio Manager is assigned before other permissions that may be assigned by groups.

Example Scenario

- A user's account is a member of **ABC-ADM Group** and **DEF-ADM Group**.
 - **ABC-ADM Group** is nested underneath the group **XYZ-NerdioSupport-Admin**.
 - **ABC-ADM Group** is assigned to workspace A with a custom role in Nerdio Manager.
 - **DEF-ADM Group** is assigned to workspace B with a custom role in Nerdio Manager.
 - **XYZ- NerdioSupport- Admin** is assigned to workspaces C and D as an AVD Admin in Nerdio Manager.
1. The nested membership plays no role. Therefore, as far as Entra ID is concerned, the **ABC-ADM Group** as a member of **XYZ-NerdioSupport-Admin** does not exist. Only users that are direct members of the **XYZ- NerdioSupport- Admin** group are considered. Since the user is not a direct member of **XYZ-NerdioSupport-Admin**, they do not have access to workspaces C or D.

2. Since the user is a direct member of both **ABC-ADM Group** and **DEF-ADM Group**, and both of those groups are assigned to a custom role, therefore, the same tier of permissions per Entra ID, then the effective permissions of the user is going to be the cumulative total of the permissions assigned to the **ABC-ADM Group** and **DEF-ADM Group**.

Feature Limitations

In this initial release of the cumulative RBAC feature, there are some functional limitations. These will be addressed in the future where possible.

- Built-in roles are not supported for this feature. Only custom roles may be used.
- The feature does not support mixing of different access levels to the workspace module across separate assignments. For example, you cannot mix the 'Manage Hosts' and 'Manage Sessions' permission in the workspaces module across separate assignments, because only one access level for the workspaces module is supported globally.
- You cannot mix limited permissions with Full Access, even when restricting the scope to specific workspaces, because the Full Access user interface would conflict with the limits set.
- You cannot mix limited permissions with Read Only, even when restricting the scope to specific workspaces, because the Read Only user interface would conflict with the limits set.
- The maximum supported number of assignments is 10. Additional assignments are filtered out.

RBAC Considerations prior to Nerdio Manager v6.4

This section discusses the situation where a user is potentially a member of different groups for environments prior to v6.4. Some of these may be direct assignments or a nested group assignment.

- The groups are assigned to different custom roles. For example, two assignments grant access to workspace A with varying custom permissions (that is, the same workspace), and one assignment grants access to workspaces B, C, and D.
- When the user signs in, they only see the workspace A. They do **not** see workspaces B, C, and D.

- In fact, you want the user to have access to all the workspaces (A, B, C, and D).

Core Permission Assignment Principles

The following are the core principles related to how the permission assignments apply through Entra ID and how Nerdio Manager interprets them.

- User assignment to Entra ID applications does not support nested group membership. That is, users can only be assigned directly to the application with a specific role and workspace combination, or they can be a direct member of a group that is assigned to the application. Assigned as both a user and group member is supported, but Nerdio Manager prioritizes the user assignment first (see below).
- Members of a group that is a nested member of another group, which is assigned to the Entra ID application, are not considered. This is an Entra ID limit. See this Microsoft [article](#) for details.
- Nerdio Manager's built-in default roles are arranged in order of tiers with decreasing permission. If a user is a member of groups with multiple equivalent role tiers, then Entra ID only provides one of those assignments to Nerdio Manager. In general, it is provided alphabetically, so the first alphabetical group's assignments apply in most situations, but technically it can be processed in any order.

Additional Principles

- All custom roles created in Nerdio Manager are considered to be the same tier in terms of Entra ID's role permissions. Nerdio Manager can not merge or consolidate permissions to enable access to the most permissive combination.
- Even if there was a custom role that enables all permissions, and a second role that only includes a single permission, because they are both considered to be a custom role, they are equal on the same tier from the perspective of the Azure application.
- A direct user assignment is considered the highest priority. Therefore, any user directly assigned to Nerdio Manager bypasses any alternate permissions that may be assigned by group. However, users should only have a single assignment, otherwise it is subject to the same processing challenges as multiple group memberships.

Example Scenario

- A user's account is a member of **ABC-ADM Group** and **DEF-ADM Group**.
 - **ABC-ADM Group** is nested underneath the group **XYZ-NerdioSupport-Admin**.
 - **ABC-ADM Group** is assigned to workspace A with a custom role in Nerdio Manager.
 - **DEF-ADM Group** is assigned to workspace B with a custom role in Nerdio Manager.
 - **XYZ-NerdioSupport-Admin** is assigned to workspaces C and D as an AVD Admin in Nerdio Manager.
1. The nested membership plays no role. Therefore, as far as Entra ID is concerned, the **ABC-ADM Group** as a member of **XYZ-NerdioSupport-Admin** does not exist. Only users that are direct members of the **XYZ-NerdioSupport-Admin** group are considered. Since the user is not a direct member of **XYZ-NerdioSupport-Admin**, they do not have access to workspaces C or D.
 2. Since the user is a direct member of both **ABC-ADM Group** and **DEF-ADM Group**, and both of those groups are assigned to a custom role (therefore, the same tier of permissions per Entra ID), then the effective permissions of the user is going to be a toss up between what workspaces/pools those groups are assigned to. In this example, that is either workspace A or workspace B.
 3. Typically, the assignment is done alphabetically, but there is no official definition of how that is interpreted by Entra ID. Therefore, today, the user could see the workspace A that is enabled by **ABC-ADM Group**. Tomorrow, the user may see workspace B that is enabled by **DEF-ADM Group**. Entra ID makes the evaluation and provides the user with access to Nerdio Manager under that group. Nerdio Manager just sees that a member of a specific group has signed in, and grants the permissions accordingly.

**Note**

This could also apply to two different RBAC role assignments in Nerdio Manager, where two different groups are assigned to the same workspace (for example, workspace A), but have two different custom role definitions. One assignment may be grant permissions to one set of host pools, while the other group may be assigned to a different set of host pools.

Because all custom roles are on an equivalent tier, the specific host pools visible to the user may change depending on which group evaluation Entra ID makes when signing in to Nerdio Manager.

Recommendations

**Tip**

Be sure to follow these recommendations to ensure a clear and consistent experience.

- **Option #1:** Either modify the group membership or assignments used to grant the user access to Nerdio Manager, so that there is only one group membership applied with a single custom role granting access to all the requisite workspaces that the user should have entitled.

**Note**

Not having multiple groups for Entra ID to evaluate ensures only the single correct assignment is applied.

- **Option #2:** Assign the user's account explicitly, not as group membership, to the custom role directly, and grant access to all workspaces that should be entitled.



Note

Having a single direct assignment ensures that the exact required permissions are applied.



Tip

While either solution would work, we would recommend using Option #1. This helps prevent bloating the permission listing with a large number of individual users.