Nerdio Manager for Enterprise Implementation Guide

Last Revised: December 2024

Table of Contents

Copyright

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

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

Introduction

This document is designed to help you implement Nerdio Manager efficiently and effectively.

This is a highly-focused document that enables you to get Nerdio Manager up and running. It only touches on the features you need to implement Nerdio Manager. You can see all of Nerdio Manager's features on our support website.

Of course, we are here to help with your implementation. If you need help, please send the support team an email (nme.support@getnerdio.com).

Step #1: Installation

The first step, obviously, is to install Nerdio Manager.

Azure Permissions and Nerdio Manager

Nerdio Manager is an Azure application that is deployed from the Azure Marketplace and runs inside your own Entra ID tenant and Azure subscription. It requires certain permissions during installation, configuration, and ongoing use.

Tip: See the following document for a deep dive into the Azure permissions and Nerdio Manager: Nerdio Manager for Enterprise - Permissions.

Installation Permissions

The Entra ID user performing the installation of Nerdio Manager requires the following permissions:

- **Global Administrator** role in Entra ID.
- **Owner** role in the Azure subscription.

Note: These elevated permissions are needed only for the initial installation and configuration process, and are not necessary for the ongoing use of Nerdio Manager.

When Nerdio Manager is installed, it has the following API application permissions in Azure:

Service	Permission	Function
Azure Resource Manager	Subscription Reader Subscription Backup Reader	List the available resources in the Azure subscription and make requests on behalf of the user.

Service	Permission	Function
Microsoft Graph	Application.Read.All (delegated) AppRoleAssignment.ReadWrite.All (delegated) Application.ReadWrite.All (delegated)	Manage the Nerdio Manager application service principal and assign the users to the Nerdio Manager application to enable user sign in.
Microsoft Graph	Organization.Read.All (delegated) Organization.Read.All (application)	Read organization-level information, such as tenant name.
Microsoft Graph	User.Read (delegated) User.ReadBasic.All (delegated) User.Read.All (application) User.Read.All (delegated) Group.Read.All (application) Group.Read.All (delegated) GroupMember.Read.All (delegated)	Read the Entra ID groups and membership for app group assignments.
Microsoft Graph	Offline_access (delegated) Openid (delegated) profile (delegated) (Optional) Mail.Send (delegated)	Allow user sign in and delegated actions.
Azure Service Management	user_impersonation (delegated)	Make requests to Azure on behalf of the user.

Service	Permission	Function
Windows Virtual Desktop	TenantCreator (application)	(AVD Classic/V1) Create the AVD tenants.
Windows Virtual Desktop	user_impersonation (delegated)	(AVD Classic/V1) Make requests on behalf of the user.

Note: `Group.Read.All` and `User.Read.All` application-level API permissions can be removed in version 4.0 and later. Removing these permissions has the following implications:

- REST API cannot be used to assign users to host pools without `User.Read.All` application-level permission.
- If using Installed Apps management with existing rulesets, after removing `Group.Read.All` application-level permissions, be sure to open each ruleset and save it.

Subscription Permissions

While activating Nerdio Manager licensing subscription, a new SaaS subscription object Azure resource is created on the Azure subscription, which allows Nerdio Manager to charge for license consumption as a 3rd party service on the Azure bill. In order to configure a SaaS subscription object, because it causes additional costs to be included on the subscription, the user completing the configuration must be a **subscription owner**.

A new Entra ID application registration specific for Nerdio Manager's billing is also created automatically as part of the resource deployment. This application is granted the below permissions in order to authenticate as your user on behalf of your Azure tenant, and register the SaaS subscription object as being tied to your Azure subscription. These permissions allow the billing application to inform Nerdio Manager's licensing service the following details:

- Who is completing the purchase.
- Which SaaS subscription object is used for billing.
- Which Entra ID tenant you are connecting from.

Note: These are the same permissions being granted to the billing application as are granted to the primary Nerdio Manager application above.

Service	Permission	Function
Microsoft Graph	openid, profile, User.Read (delegated)	Allows user sign in (name & Azure tenant ID are shared).

Configuration Permissions

Once the Nerdio Manager application is installed, there are several configuration actions that can be taken inside of Nerdio Manager to "link" it to existing Azure resources or create new ones. These actions require the requesting user (that is, the user signed in and performing the action via Nerdio Manager) to have certain permissions on the Azure resources that are being used.

Action	Permissions Required
Link a resource group	The requesting user must be an Owner on the resource group being linked.
Link a network	The requesting user must be an Owner on the vNet that is being linked (or the resource group that contains the vNet).
Link an additional Azure subscription	The requesting user must be an Owner on the subscription that is being linked.
Switch the AVD object model from Classic to ARM	The requesting user must be a Global Administrator in the Entra ID in order to

Action	Permissions Required
	grant the required admin consent.
Enable Sepago Azure monitoring	The requesting user must be an Owner on the selected resource group for deployment of the Log Analytics resources and permission assignment.
Create Azure Files shares	The requesting user must be a Contributor on the selected resource group for the storage account deployment. To join a newly created Azure Files share to Active Directory, the selected AD profile must have permissions to create ServicePrincipalName objects (See Permissions Required to Join Azure Files Share to Domain (Active Directory) for additional details.)
Create Azure NetApp Files volumes	The requesting user must be a Contributor on the selected resource group for NetApp account deployment and the vNet containing the NetApp Files subnet.
Create AVD ARM host pools	The requesting user must be a Contributor on the resource group in which the host pool is being created. To allow Nerdio Manager to manage app group membership, the requesting user must be an Owner on the resource group into which the host pool and app group are being deployed.
Add access to the Nerdio Manager for other users	The requesting user must be an AVD Admin in Nerdio Manager.

Action	Permissions Required
Associate session host VMs from previous AVD deployment	The requesting user must be a Contributor in the resource group that contains the VMs.

Ongoing Use Permissions

When the Nerdio Manager application is installed and configured, no user permissions in Azure are required to manage the configured AVD environment via Nerdio Manager. Most actions in Nerdio Manager run on Nerdio Manager on behalf of the signed in user.

Note: There are several RBAC roles available. See Role-based Access Control (RBAC) in NME for details.

Nerdio Manager Installation Guide

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

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

Nerdio Manager is installed and billed through the Azure Marketplace.

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

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

Companion Video

Prerequisites

Note: Sign in to your Azure portal as a Global Administrator before starting the install process.

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

installation, and Nerdio Manager can create Azure Files or NetApp Files after the installation.

- The Microsoft Desktop Virtualization resource provider must be registered in your Azure subscription.

Install Nerdio Manager from the Azure Marketplace

Nerdio Manager is installed from the Azure Marketplace.

To install Nerdio Manager:

1. In the Azure Marketplace, search for Nerdio Manager for Enterprise.
2. Select **Create** > **NME Plan** to start the installation process.
3. Enter the following information:
    - **Subscription**: From the drop-down list, select the subscription where you want to install Nerdio Manager.
    - **Resource Group**: Select **`Create new`** to create a new resource group.
    - **Region**: From the drop-down list, select the region closest to you or where the majority of your administrators are located.

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

4. Once you have entered all the desired information, select **Next: Review + create**.
5. Review your selections and select **Create**.

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

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

7. Locate and select the **App service.**
8. Select **Browse** or select the URL to navigate to your installation of Nerdio Manager.

Initialize Nerdio Manager

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

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

To initialize Nerdio Manager (Typical):

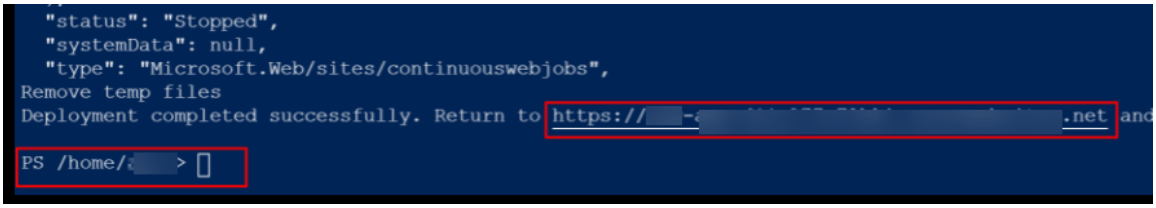
1. Sign in to the Nerdio Manager web application as the **Global Administrator** and the subscription **Owner**.
2. Select the copy button to copy the command.

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

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

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

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



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

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

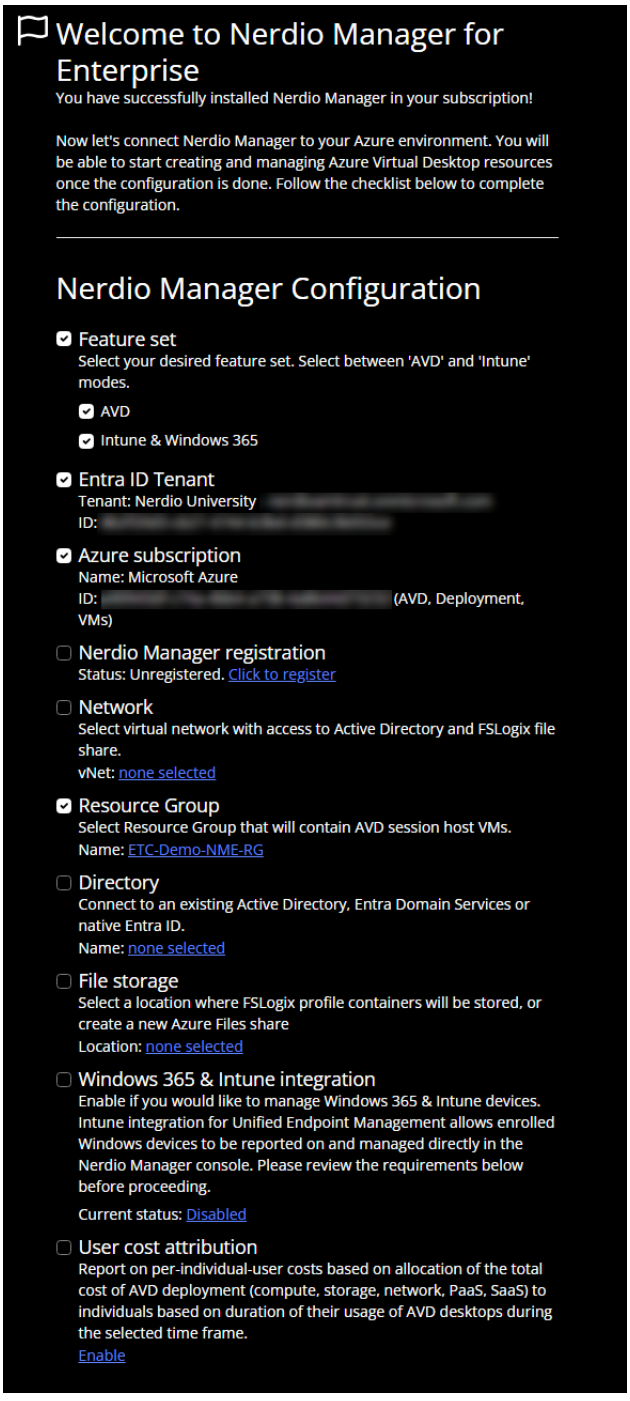
1. Sign in to the Nerdio Manager web application as the **Global Administrator** and the subscription **Owner**.
2. Select **Show advanced**.
3. For Entra ID app registration:
    - **Use existing Entra ID app registration**: Select this option.
    - **App ID**: Type the App ID.
    - **App Secret**: Type the App secret.
    - **Service Principal ID**: Type the service principal ID.
4. For Split Identity:
    - **Split Identity**: Select this option.
    - **Identity Tenant ID**: Type the identity tenant ID.
5. Select **`Download script (Az)`**.
6. From your local machine, locate and run the downloaded script.

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

Configure Nerdio Manager Settings

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

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



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

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

To configure the Nerdio Manager settings:

1. In the **Feature set** section, select your desired feature set:
    - AVD
    - Intune & Windows 365

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

2. In the **Nerdio Manager registration** section:
    - Select **`Click to register`**.
    - Enter your registration information.
    - Once you have entered all your registration information, select **`Register`**.
3. In the **Network** section:
    - Select **none selected**.
    - **Subnet**: From the drop-down list, select the subnet.
    - Select **OK**.
4. In the **Resource Group** section:

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

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

5. In the **Directory** section:

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

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

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

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

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

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

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

> **Note:** See the following Microsoft document for more information about FSLogix Cloud Cache.
>
> Cloud Cache allows you to specify multiple profile storage locations. It asynchronously replicates the profiles and makes the profiles available in multiple storage locations at the same time. So, if one of the locations is not available, the session host automatically fails over to one of the alternate locations.

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

> **Note:** For more information, see Configure the session hosts | Microsoft Learn.

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

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

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

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

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

To complete the installation process:

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

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

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

Nerdio Manager Edition Management

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

Please see our website for details about the features and pricing.

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

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

To change your edition of Nerdio Manager:

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

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

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

   Your edition of Nerdio Manager is changed.

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

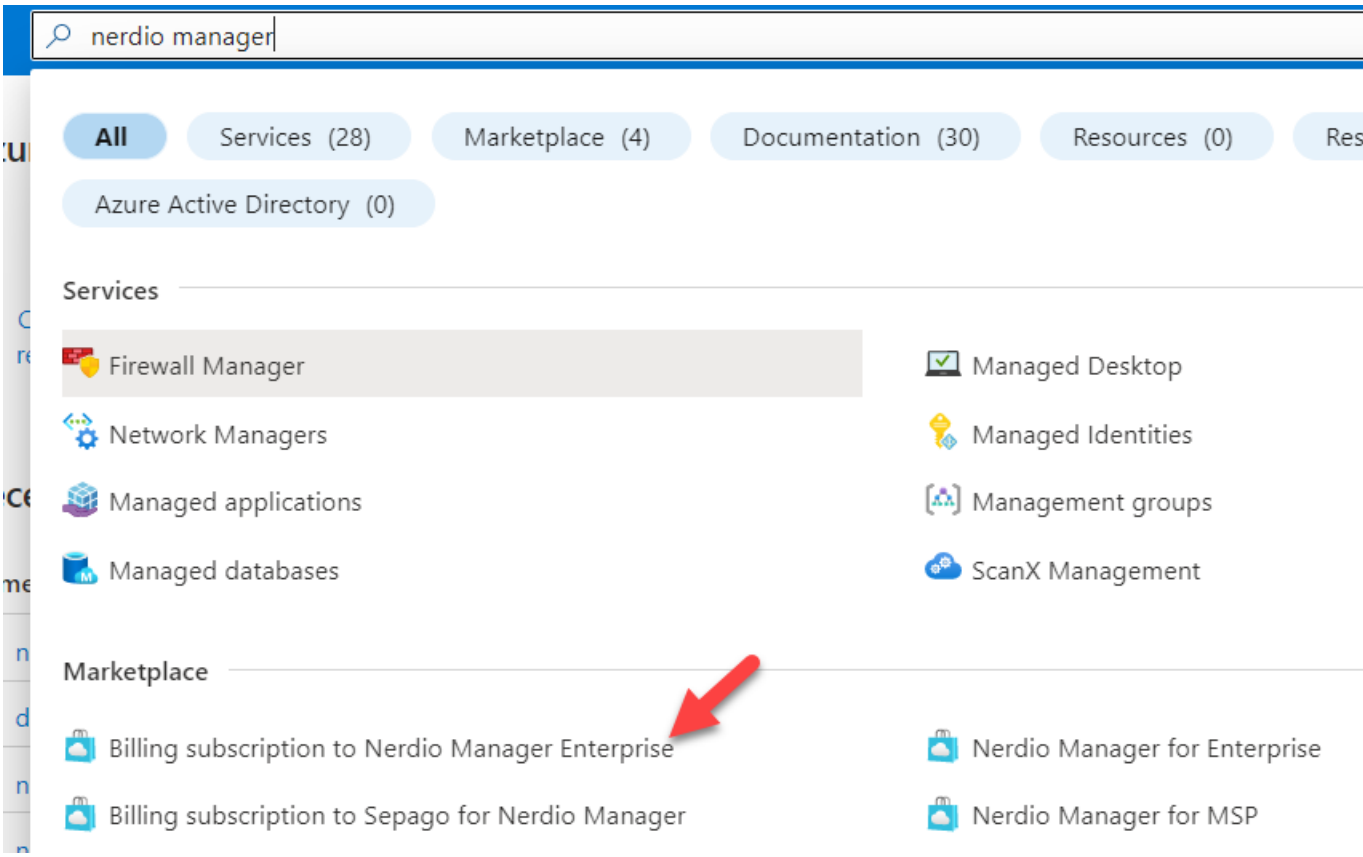
License Activation

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 the license 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. Please see "Azure Permissions and Nerdio Manager" on page 9 for additional details.

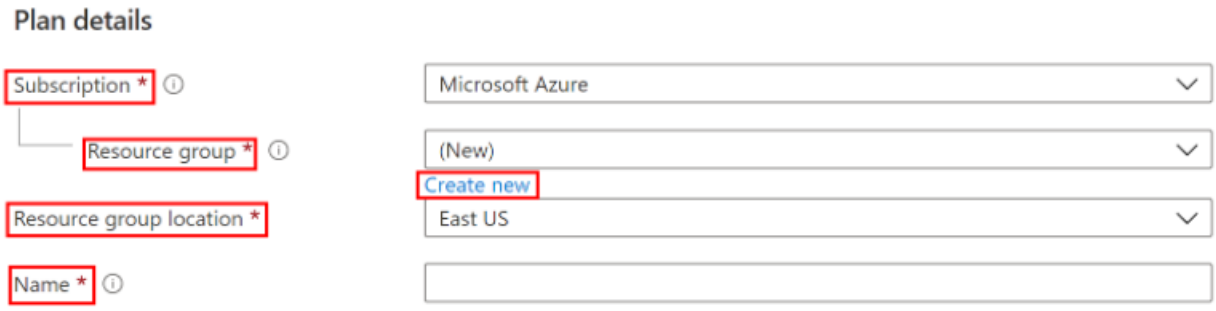
To activate the Nerdio Manager license:

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. Search for "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.



- **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**: Type "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. A **Subscription is in progress** message displays.
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.

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

You may select additional networks that you want to link to be used in Nerdio Manager. Linked networks can be selected when adding desktop images, host pools, and session hosts. The Azure region of the selected network determines the location of the VM created in this network.

You may also select additional resource groups that may contain session host VMs and desktop images.

Note: You may also set the default network and resource group. The defaults are used when creating a new desktop image, host pool, or session host. The defaults may be overridden during the creation processes.

To Add a Linked Network

1. Navigate to **Settings** > **Azure Environment**.
2. In the **Linked networks** tile, select **`Link`**.
3. Enter the following information:
    - **Subnet**: From the drop-down list, select the subnet(s).
4. Once you have entered all the desired information, select **`OK`**.

   The network(s) is (are) linked.

To Unlink a Network

1. Navigate to **Settings** > **Azure Environment**.
2. In the **Linked networks** tile, locate the network to unlink and select **`Unlink`**.
3. At the confirmation pop-up, select **`OK`**.

> **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 **Settings** > **Azure Environment**.
2. In the **Linked networks** tile, locate the network to be the default and select **`set default`**.

To Add a Linked Resource Group

1. Navigate to **Settings** > **Azure Environment**.
2. In the **Linked resource groups** tile, select **`Link`**.
3. Enter the following information:
    - **Resource group**: From the drop-down list, select the resource group(s) to link.

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

   The resource group(s) is (are) linked.

To Unlink a Resource Group

1. Navigate to **Settings** > **Azure Environment**.
2. In the **Linked resource groups** tile, locate the resource group to unlink and select **Unlink**.
3. At the confirmation pop-up, select **OK**.

> **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 **Settings** > **Azure Environment**.
2. In the **Linked resource groups** tile, locate the resource group to be the default and select **set default**.

UI Overview

Nerdio Manager's UI is feature rich and customizable.

Time Zone

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

Menu

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

Help

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

Nerdio Manager Copilot

Select the **Copilot** icon to launch the AI-assisted help system. See"Manage Nerdio Manager Copilot" on page 36 for details.

Breadcrumbs

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

Table Footer

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

Tasks

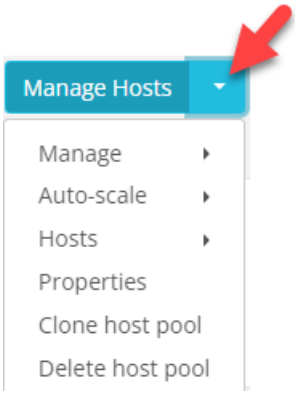
The **Tasks** section displays a log of the tasks related to the page in reverse chronological order. For example, the Workspaces page displays the log of the tasks performed on the Workspaces.

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

See Logs Module for details.

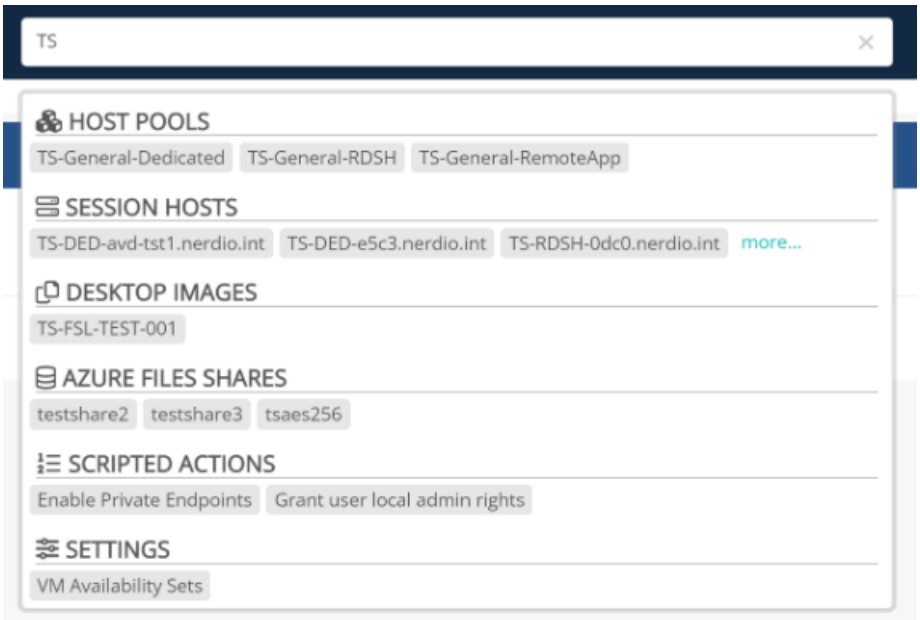
Action Menu

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



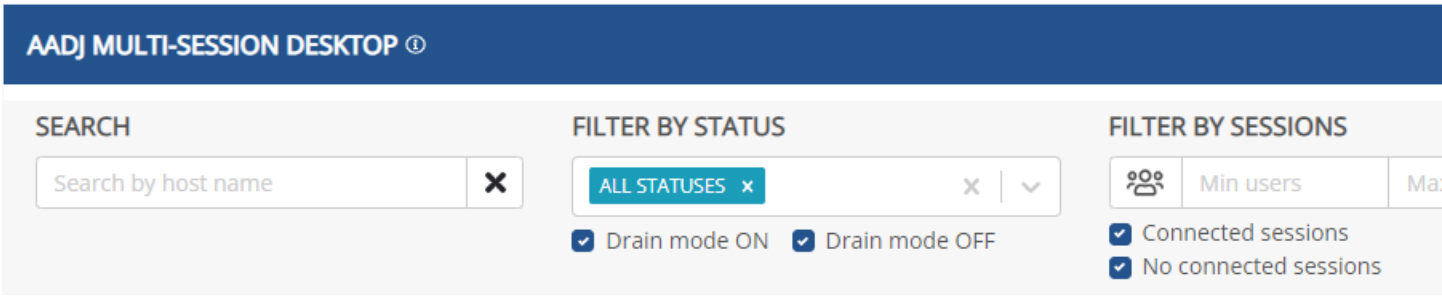
Global Search Bar

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



Search and Filter

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



Notes:

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

Refresh

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

Tool Tip

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

Sort a Table

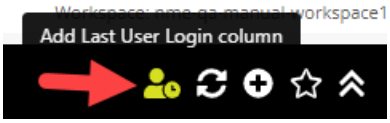
In a table column header, select the **Sort** icon to sort the table in ascending or descending order by that column.

Add New

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

Display Last Login Date

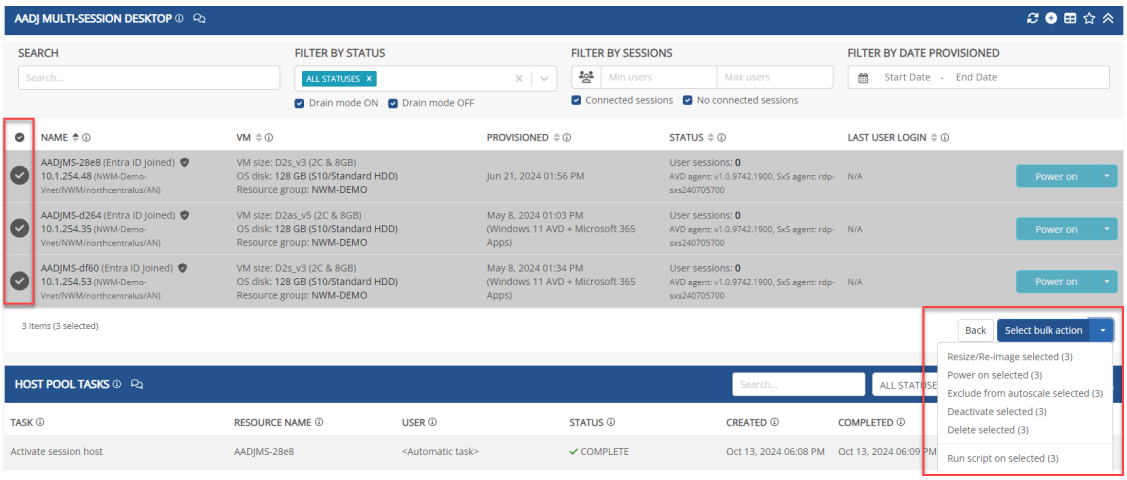
Where applicable, you can display the last login for session host VMs or user sessions. In the upper right corner, select the **Add Last User Login column** button.



Multi-select and Bulk Actions

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

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



Custom Views

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

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

See Create a Custom View for details.

Custom Views based on an Existing Page

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

See Create a Custom View from an Existing Page for details.

Individualize Your UI Themes

Nerdio Manager allows you to individualize your UI themes.

See Individualize Your UI Themes for details.

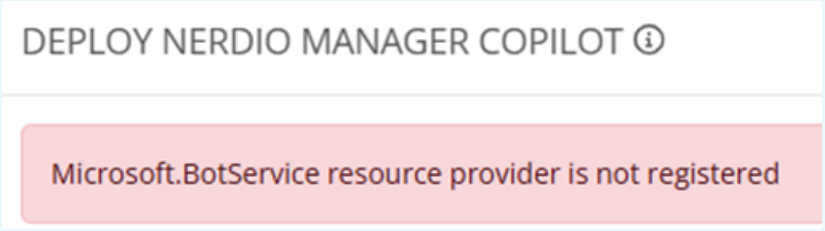
Manage Nerdio Manager Copilot

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

Enable Nerdio Manager Copilot

Notes:

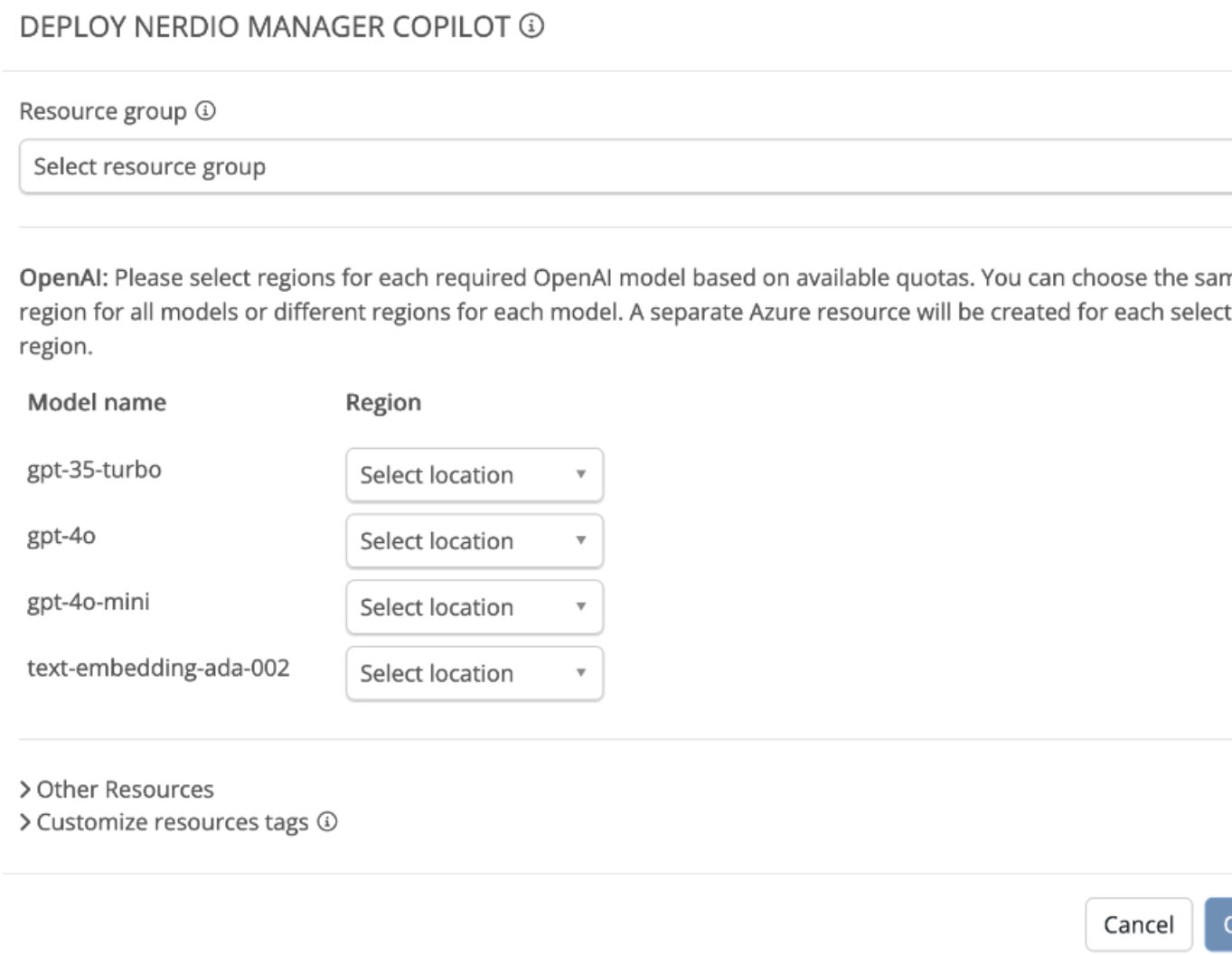
- Availability of Azure OpenAI services is limited and varies by Azure region.
- When enabling Copilot, you might have to register the following resource providers first or you might see this error message.



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

To enable Nerdio Manager Copilot:

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

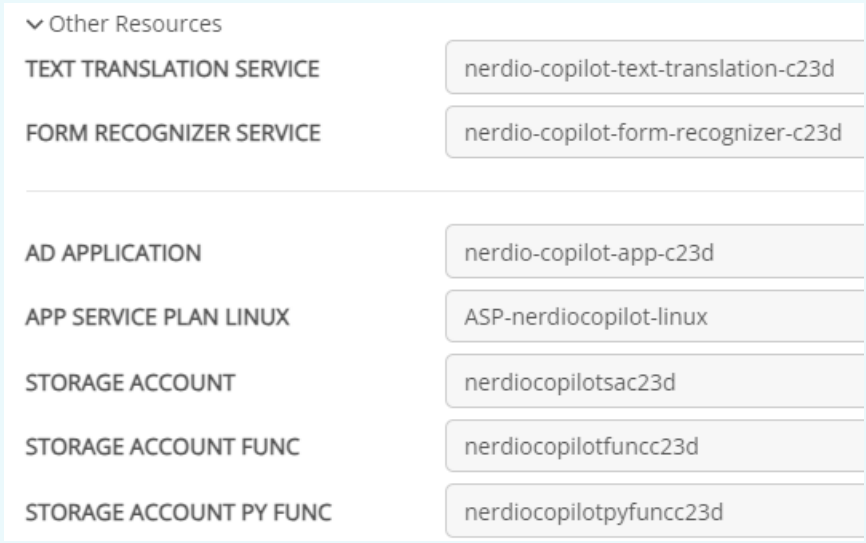


3. Enter the following information:

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

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

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

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

- **Customize resources tags**: Optionally, expand this to enter custom tags.

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

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

Use Nerdio Manager Copilot

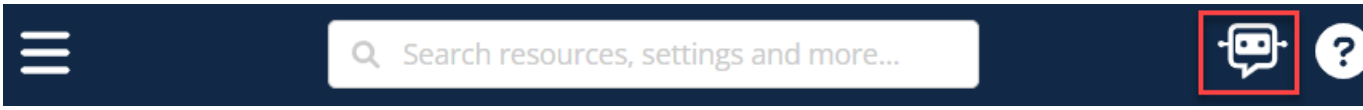
Once all Azure resources for Copilot are deployed, you may use Copilot.

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

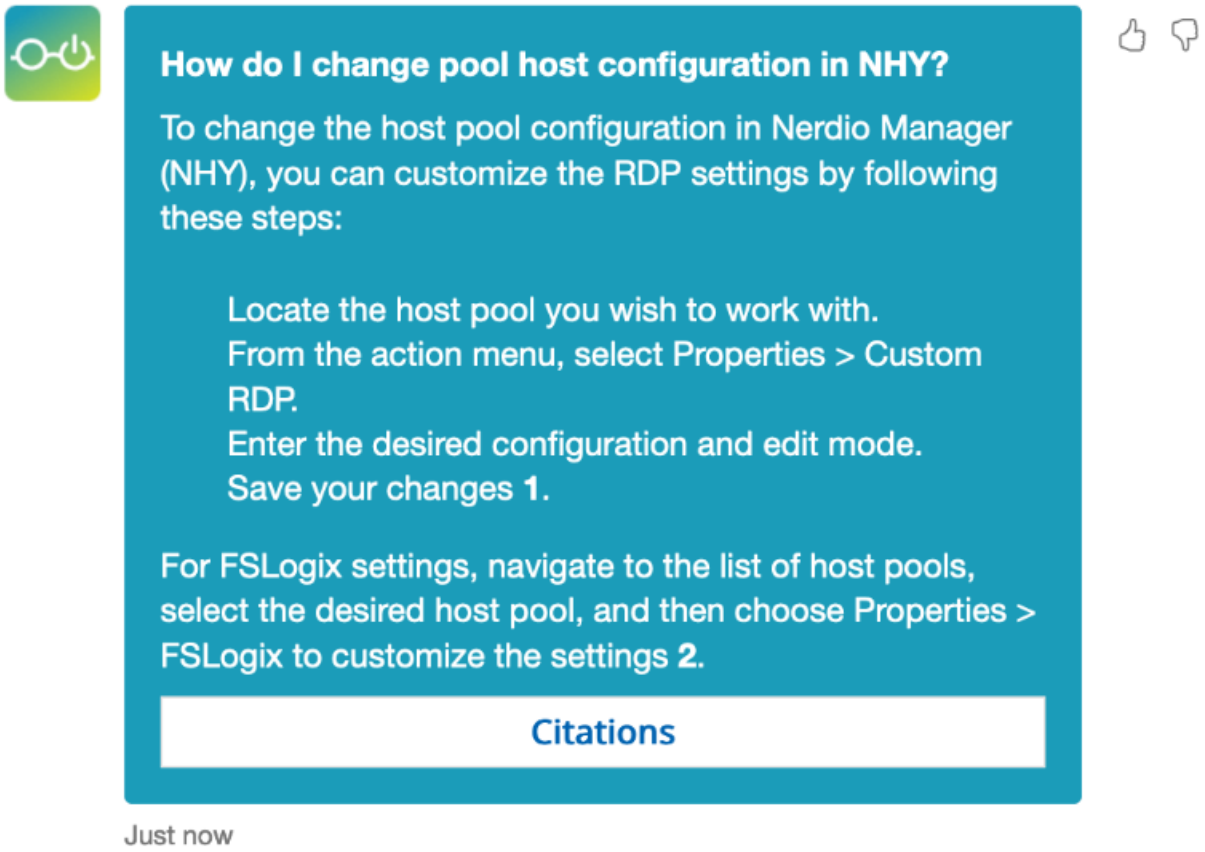
To use Nerdio Manager Copilot:

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

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



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



3. Optionally, select **Citations** to view a list of cited Knowledge Base articles.
4. You may select any of the view options:
   - Switch to Sidebar window:

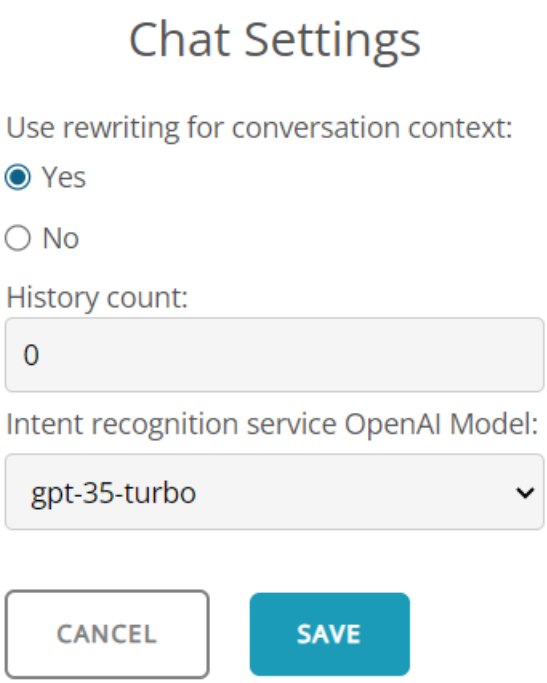
- Switch to Detached window:

Manage Nerdio Manager Copilot's Chat Settings

You may manage Copilot's settings at any time.

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

1. Select the **Settings** icon. 



2. Enter the following information:
   - **Use rewriting for conversation context**: Select **Yes** or **No**.
   - **History count**: Type the number of chat histories to retain.
   - **Intent recognition service OpenAI Model**: From the drop-down list, select the desired model.

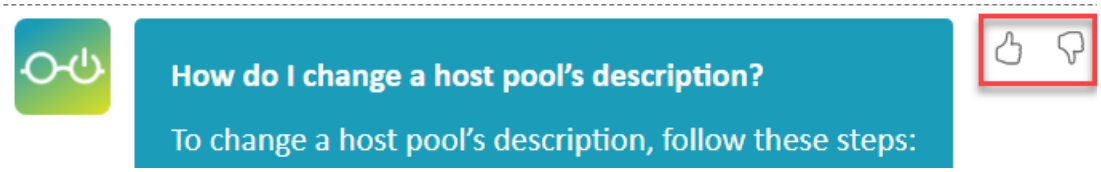
3. Once you have entered the desired information, select **Save**.
4. When prompted, select **Confirm** to confirm your changes.

Submit Feedback

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

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

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



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

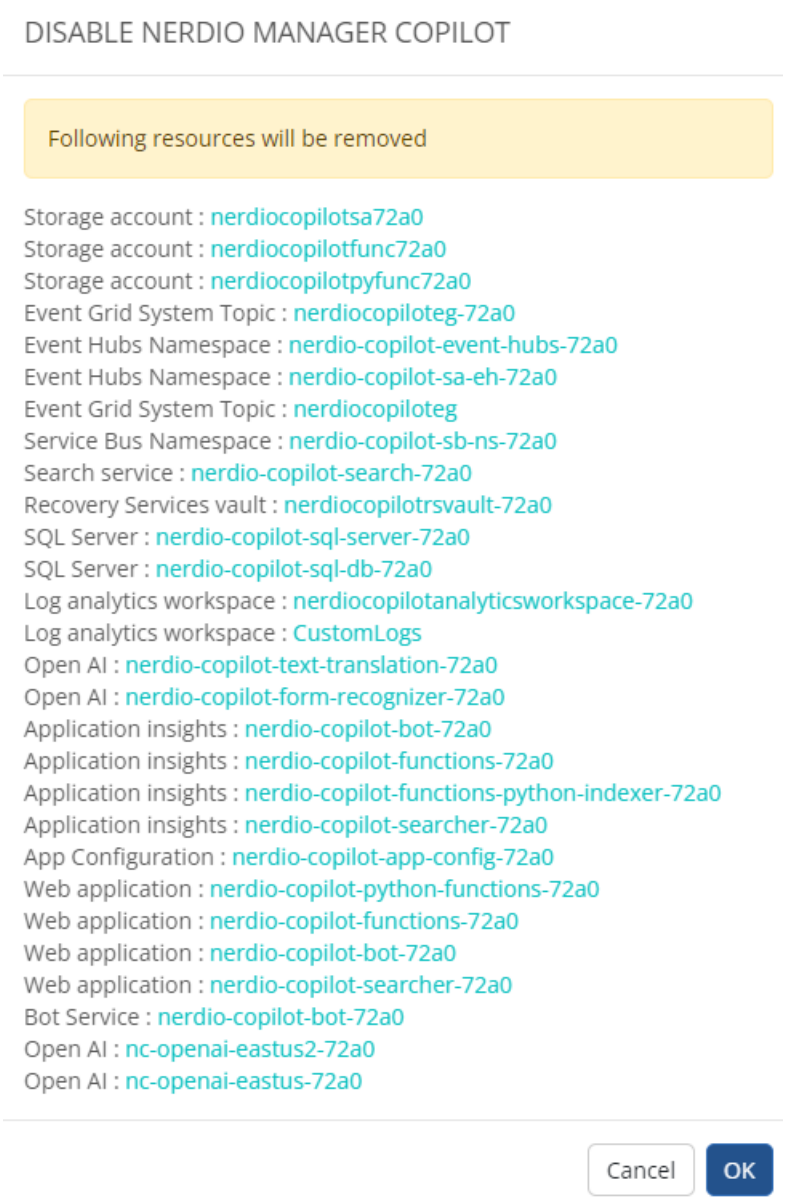
Disable Nerdio Manager Copilot

Follow this procedure to disable Nerdio Manager Copilot.

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

To disable Nerdio Manager Copilot:

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



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

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

Cost of Nerdio Manager Copilot

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

Copilot has the following paid components:

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

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

- **App Service**: The price depends on the App Service plan that Nerdio Manager Copilot is using. The default plan is B2 (Linux). See the following Microsoft article for more details.
- **Azure OpenAI Service**This service's cost depends on usage of Copilot and the number of input and output tokens that are being used in each interaction. See the following Microsoft article for more details.
- **Azure AI Search**: Copilot uses the basic tier for this service that is priced at $0.11 per hour , which is approximately $80 per month. See the following Microsoft article for more details.
- **Azure Event Grid**: The Event Grid Basic tier is priced as pay-per-use based on operations performed. The detailed pricing info is here.

- **Azure Event Hub**: The basic tier pricing starts from $0.015/hour per Throughput Unit (about $12/month). The detailed pricing info is here.
- **Azure Service Bus**: The basic tier pricing starts from $0.05 per million operations. The detailed pricing info is here.
- **Azure SQL**: Standard service tier (S0), Max storage: 250 GB, which is about $14.7187/month
- **Azure App Configuration**: In Standard tier, this service charges $1.20 per store per day, plus an overage charge at $0.06 per 10,000 requests. The monthly charge expects to be no more than $36. See the following Microsoft article for more details.
- **Azure Text Translation**: This uses tier S1 – Pay as you go (Standard Translation - $10 per million characters, Custom Translation - $40 per million characters). Here is the pricing page.
- **Azure Form Recognizer**: This uses tier S0 - Pay as you go (minimal charge is: 0-1M pages - $1.50 per 1,000 pages, 1M+ pages - $0.60 per 1,000 pages). Here is the pricing page.
- **Azure Bot Service**: The free tier is used. Detailed pricing info is here.
- **Azure Functions**: The Azure Functions consumption plan is billed based on per-second resource consumption and executions. The detailed pricing page with calculation examples is here.
- **Azure Storage**: Some of the components use Azure Storage. The cost of storage varies depending on the region and access tier selected, as well as the type of storage being used. Copilot uses Azure General Purpose v2 Storage Account, locally redundant storage (LRS). Here is the pricing page.

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

Functional Considerations

LLM implementation work with tokens. The number of tokens is a combination of system prompt, input from user, and output from LLM. The number of tokens defines how much “memory” about a previous exchange in the current conversation the bot has. If a conversation is long, larger than

the max token count configured for the model, older data is dropped. However, we expose all the chat history in the UI until the chat history is deleted using the delete history button.

Deployment Considerations

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

Known Limitations

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

Manage Schedules for Tasks

Nerdio Manager supports the ability to configure schedules for tasks.

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

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

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

- **Desktop Images**: Run scripted action
- **Scripted Actions**: Run Azure Runbook
- **Host Pools**: Resize or re-image, Power on/off, Restart hosts, Send message, Log off all hosts, Activate/Deactivate hosts, Run scripted action

- **Session Hosts** (Excluding hybrid): Resize or re-image, Power on/off, Restart hosts, Send message, Activate/Deactivate hosts, Run scripted action
- **Advisor**: Resize session host, Resize host pool

Create Multiple Schedules for a Task

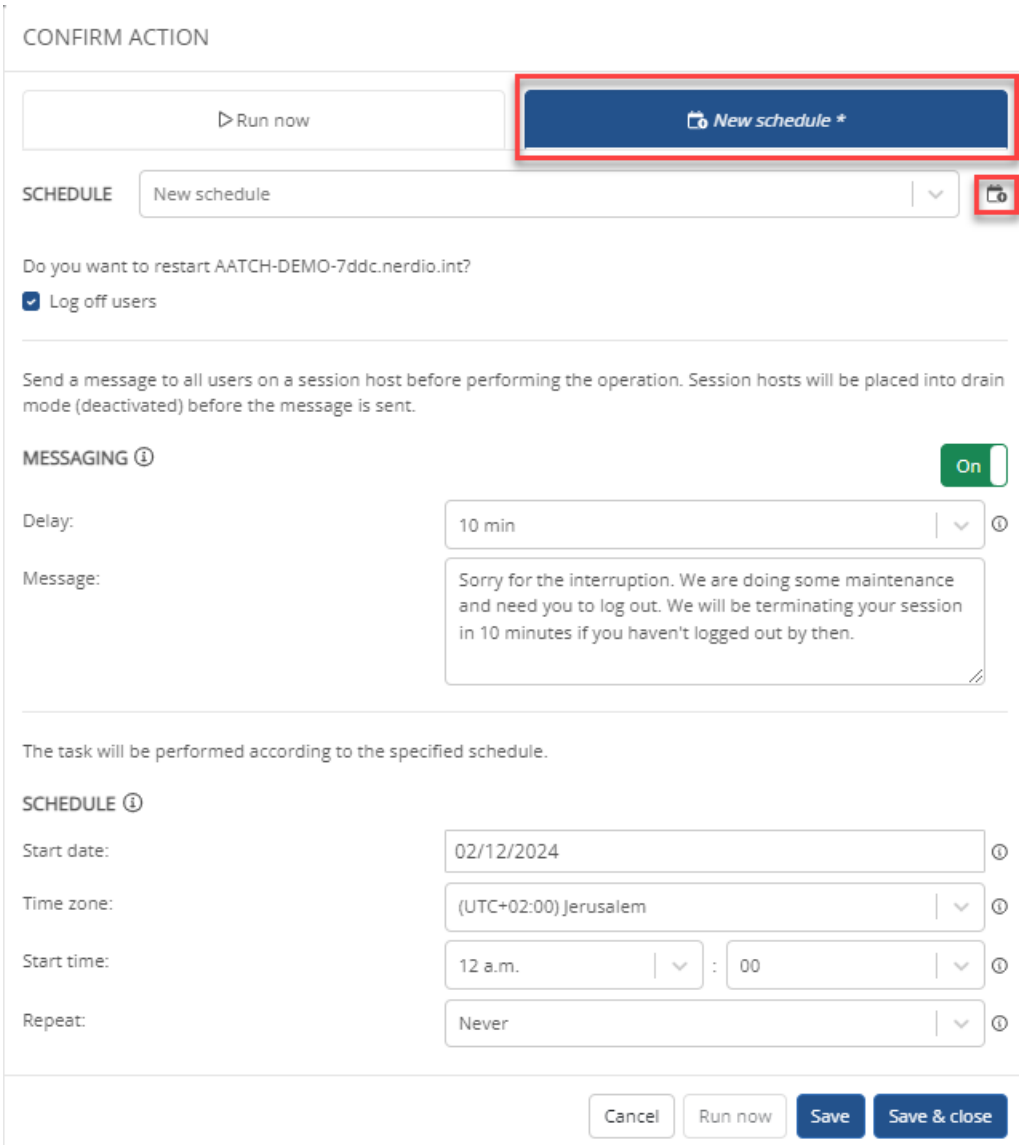
Nerdio Manager allows you to create multiple schedules for a number of tasks.

To create multiple schedules for a task:

1. Navigate to the task you wish to perform.

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

2. Select the **Schedule** tab.

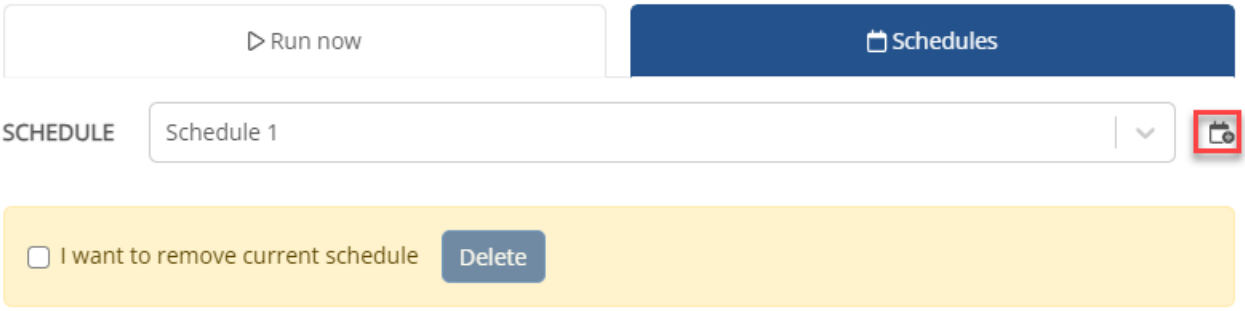


3. In the **Schedule** section, enter the desired schedule.
    - **Start Date**: Type the date to start.
    - **Time Zone**: From the drop-down list, select the time zone for the Start time.
    - **Start Time**: From the drop-down lists, select the time to start.
    - **Repeat**: From the drop-down 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.

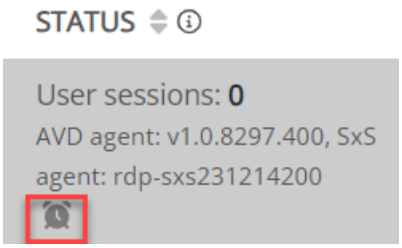
5. If you want to add additional entries, at the top, to the right of **Schedule**, select the **Add Schedule** icon.
6. Add and save the next schedule, and repeat for all the desired schedule entries.

Manage Task Schedules

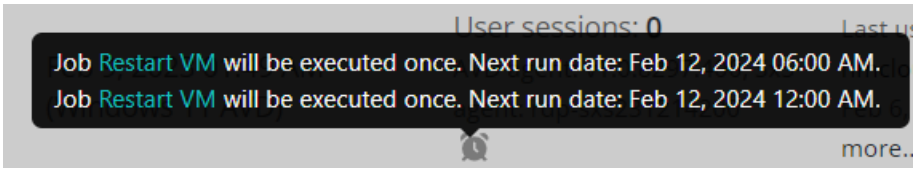
Nerdio Manager allows you to manage task schedules. This includes changing and deleting schedule entries.

To manage task schedules:

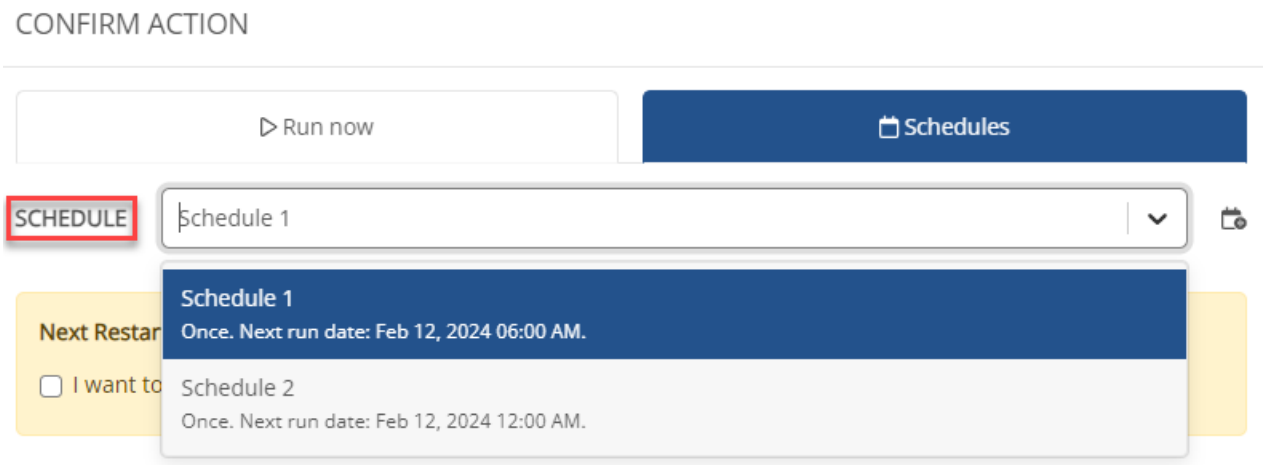
1. Navigate to the task with the schedule that you wish to work with.
2. On the list (for example, hosts, host pools, etc.), select the **Schedule** icon.



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** tab, 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**.

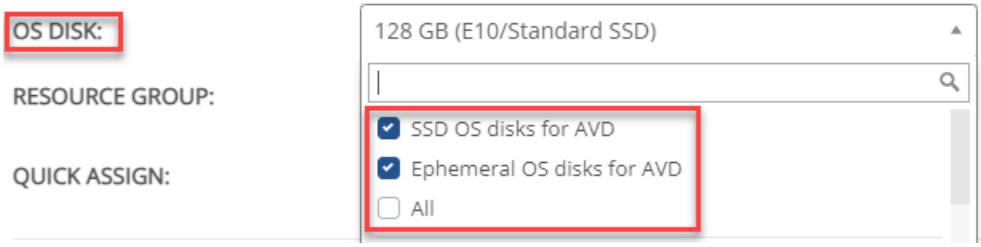
Resource Selection Rules Management

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.

Notes:

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

- **Show costs**: From the drop-down list, select **Yes** to display the monthly cost, instead of the size tier, in the VM Size drop-down list.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   The resource selection rule is created.

Manage Resource Selection Rules

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

- **Edit**: Edit the rule.

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

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

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

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

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

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

Step #2: Desktop Images

Once you have installed Nerdio Manager, the next step is to load desktop images.

Desktop Images

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

After creating a new Workspace, the next step in building out an AVD environment is to create one or multiple host pools housing your virtual machines (see "Host Pools" on page 76 for more information). Virtual machines are created based on a desktop image, which holds the operating system, your applications, and anything else you might want to add. For this to work, we first need to create at least one desktop image.

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

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

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

Management and Lifecycle Tasks for Imported Desktop Images

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

Typical Desktop Image Lifecycle

1. Import the desktop image.

   See any of the following for detailed information:

   - "Import Images from the Azure Library" on page 62
   - "Import Custom Azure Managed Images" on page 62
   - "Import an Existing VM" on page 59

2. Power on the desktop image.

   - Navigate to **Desktop Images**.
   - Locate the desktop image you wish to power on.
   - Select **Power on**.
   - Optionally, select **Back up VM before powering on**.

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

     The VM powers on.

3. Use the VM's IP address or name to connect to it using RDP and make all the desired changes.

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

   See "Desktop Images Set as Image" on page 68 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.

   See the following for detailed information.

   - "Create Dynamic Host Pools" on page 78
   - Create Static Host Pools Without Auto-Scaling
   - Resize/Re-image a Host Pool

Endpoint Management Software Integration

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

Endpoint Management Software Integration Example

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

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

- In Nerdio Manager, when you perform the **Set as image** function, be sure to select the **Leave desktop image VM running** option. This leaves the VM running after the **Set as**

image task completes and the endpoint management tool can access the VM and change the image.

- In the endpoint management tool, create a recurring scheduled job/runbook on Patch Tuesday to apply the Windows Updates.
- In Nerdio Manager, configure the **Set as image** function for the desktop image to be a recurring job that starts shortly after the endpoint management tool's job completes. See "Desktop Images Set as Image" on page 68 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.

Import an Existing VM

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

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

To import an image:

1. In Azure, navigate to the virtual machine.

   Warning: Make sure that the VM is powered off.

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

4. Select **`Generate URL`**.

   The URL is generated.

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

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

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

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

Notes:

- Security type refers to the different security features available for a virtual machine. Security features like Trusted Launch and Confidential virtual machines improve the security of Gen2 VMs. However, additional security features have some limitations, which include not supporting back up, managed disks, and ephemeral OS disks. See the following Microsoft articles for more information:
- Trusted launch for Azure virtual machines
- About Azure confidential VMs
    - If you select **Standard**, **Trusted launch virtual machines**, or **Confidential virtual machines**, then the desktop image and session host VMs are created with the specific security type.
    - If you select one of the **xxxx supported** options, then the desktop image is created as Standard but the session host VMs can be deployed as Standard or the supported type(s). (Trusted Launch and/or Confidential)

- **Uninstall FSLogix app**: Select this option if the FSLogix app is already installed in the base image and you want to remove it in order to allow Nerdio Manager to manage FSLogix.
- **Uninstall AVD agent**: Select this option if you are creating an image from an existing AVD session host where the AVD agent has been previously installed.
- Enter the information for the other fields. See "Import Images from the Azure Library" on the next page for detailed information.

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

   The desktop image import task starts.

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

Import Custom Azure Managed Images

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

To import an Azure custom image:

1. Navigate to **Desktop Images**.
2. Select **`Add from Azure library`**.
3. Enter the following information:
    - **Azure Image**: From the drop-down list, select the desired image.

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

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

    - Enter the information for the other fields. See "Import Images from the Azure Library" below for detailed information.
4. Once you have entered all the desired information, select **`OK`**.

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

Import Images from the Azure Library

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

To import an image from the Azure library:

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

3. Enter the following information:

> **Note:** For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 50 for details.

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

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

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

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

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

Note:

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

- **Secure Boot**: Select this option to enable Secure Boot, which helps protect your VMs against boot kits, rootkits, and kernel-level malware.
- **vTPM**: Select this option to enable Virtual Trusted Platform Module (vTPM), which is TPM 2.0 compliant and validates your VM boot integrity apart from securely storing keys and secrets.
- **Integrity Monitoring**: Select this option to enable cryptographic attestation and verification of VM boot integrity along with monitoring alerts if the VM didn't boot because the attestation failed with the defined baseline.
- **OS State**: From the drop-down list, select the OS state.

Note:

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

- **Join to AD**: Deselecting this means the VM is not joined to AD during the creation process. This prevents AD GPOs from applying to the image before it is created. Be sure to specify local administrator credentials below to be able to connect to the VM, since it won't be a member of the AD domain.
- **Do not create image object**: Select this option to only create a desktop image VM but not create an image object.

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

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

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

- **Enable time zone redirection**: Select this option to enable time zone redirection on the image. This allows each user to see their local device's time zone inside of their AVD desktop session.
- **Set time zone**: Select this option to set the time zone of the VM and then, from the drop-down list, select the time zone.
- **Install MSIX app attach certificates**: Select this option to install all the stored certificates on the VM, if applicable.

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

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

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

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

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

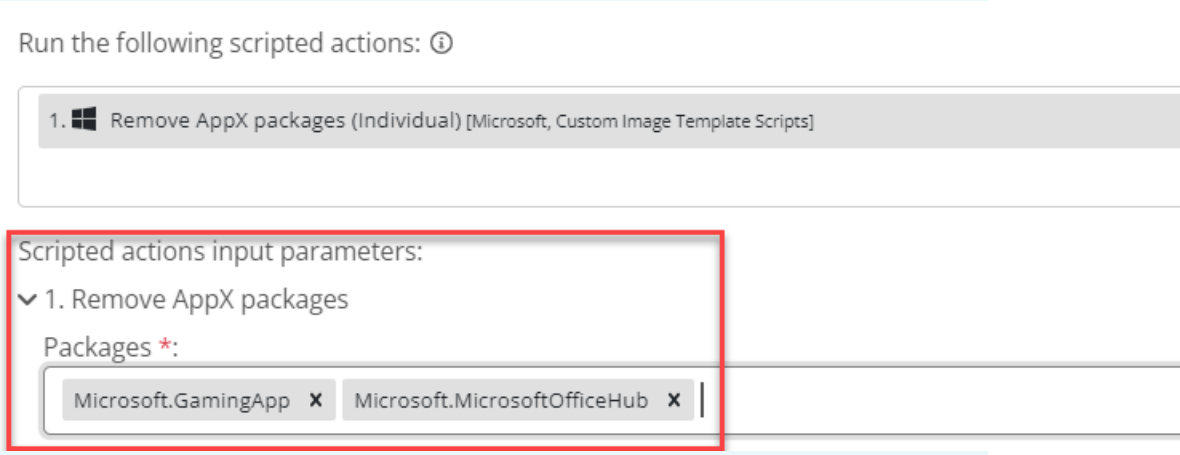
    - **Custom (Stack HCI) Locations**: From the drop-down list, select custom locations where the desktop image should be replicated.
    - **Replica Count (Per Region)**: Type number of replicas per region.

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

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

Notes:

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



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

Notes:

- You may add as many applications as desired.
- Drag and drop an application in the list to change its order on the list.
- Select the "X" next to an application to remove it from the list.

- **Install/Uninstall**: Select whether the deployment policy should install or uninstall the selected applications.
- **Reboot after installation**: Select this option to place the host in drain mode and restart it when no sessions are present.
- **Show favorites only**: Select this option to only display applications marked as favorites. Otherwise, you may search the list of applications.

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

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

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

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

Desktop Images Set as Image

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

To set a desktop image:

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

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

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

          > **Notes:**
          >
          > - You may add as many applications as desired.
          > - Drag and drop an application in the list to change its order on the list.
          > - Select the "X" next to an application to remove it from the list.

        - **Install/Uninstall**: Select whether the deployment policy should install or uninstall the selected applications.
        - **Reboot after installation**: Select this option to place the host in drain mode and restart it when no sessions are present.

  - **Show favorites only**: Select this option to only display applications marked as favorites. Otherwise, you may search the list of applications.

- **Schedule**: Toggle on the Schedule to perform the operations at a selected time(s). See "Manage Schedules for Tasks" on page 46 for details about creating a schedule.
- **Security type**: From the drop-down list, select the security option that best suits your desktop image VM.

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

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

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

- **Geographic distribution & Azure compute gallery**: Select this option to store the image in Azure Compute Gallery and automatically distribute it to the selected Azure

regions.

- **Azure Compute Gallery**: From the drop-down list, select an existing Azure Compute Gallery or create a new one.

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

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

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

- **Custom (Stack HCI) Locations**: From the drop-down list, select custom locations where the desktop image should be replicated.

- **Stage new image as inactive**: Select this option to create the new image version without setting it as active.

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

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

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

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

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

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

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

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

- **Change log**: Type the list of changes made to the image.

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

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

Desktop Images Scripted Actions

Nerdio Manager enables you to execute scripts on desktop images.

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

To execute a scripted action:

1. From the main menu, select **Desktop Images**.
2. From the action menu, select **`Run script`**.
3. Enter the following information:
    - **Schedule**: Toggle to turn the scheduler **`On`**/**`Off`**. See "Manage Schedules for Tasks" on page 46 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

Once you have created some desktop images, the next step is to create host pools.

Host Pools

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

After you create the desktop images, the next step in the Nerdio Manager AVD deployment flow is to create host pools from the desktop images.

Host pools are groups of identical Azure VMs that host the Azure Virtual Desktops that end users sign in to. All VMs in the host pool share a set of configuration options: VM size, OS disk size, base image, AD domain, user profile storage location, and more.

You can configure two types of host pools:

- **Static**: A static host pool contains a set number of session hosts that the administrator configures. That is, it does not have auto-scale enabled.

  Note: When Nerdio Manager is first deployed to an **existing** environment, the host pools that are created are static host pools. They can be converted to dynamic host pools.

- **Dynamic**: A dynamic host pool is a host pool whose configuration can be scaled in and out (auto-scale) as per the workload. That is, auto-scale can create the session hosts automatically based on the auto-scale configuration.

Related Topics

"Create Dynamic Host Pools" on page 78

Workspace Management

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.

A workspace is a container for host pools and session hosts that provide desktops and RemoteApps to users. This topic discusses creating and managing workspaces.

Create a Workspace

A workspace must be created before you can create host pools and session hosts.

To create a workspace:

1. Navigate to **Workspaces**.
2. Select **Add Workspace**.
3. Enter the following information:
    - **Name**: Type the workspace's name.

      Note: The Name is assigned to the workspace during creation and cannot be changed later. By default, it is visible to the end-user. Specifying a Friendly Name overrides what is visible to the end-user.

    - **Friendly Name**: Type the Friendly Name.
    - **Description**: Type the description, which is only visible to admins.
    - **Resource group**: From the drop-down list, select the resource group to contain the workspace.

- **Location**: From the drop-down list, select the Azure location for the workspace's objects and associated metadata.
- **Apply tags**: Optionally, type the **Name** and **Value** of the Azure tag to apply to the Workspace.

> **Note:** You may specify multiple tags. See this Microsoft article for details about using tags to organize your Azure resources.

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

   The workspace is created.

Manage Workspaces

From the Workspaces table, you can do the following:

- **Dynamic host pools**: Manage the workspace's dynamic host pools.
- **Static host pools**: Manage the workspace's static host pools.
- **Unassign**: Unassign the workspace from Nerdio Manager.
- **Delete**: Delete a Workspace.

> **Note:** You may only delete a workspace that has no host pools.

- **User Sessions**: Manage the workspace's user sessions.

Create Dynamic Host Pools

> **Warning:** Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

The following procedure allows you to create a new dynamic host pool.

To create a new dynamic host pool:

1. Navigate to **Workspaces**.
2. Select the workspace you wish to work with.
3. Navigate to **Workspaces** > **Dynamic Host Pools**.
4. Select **Add dynamic host pool**.
5. Enter the following information:

> **Note:** For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 50 for details.

- **Name**: Type the name of the host pool.
- **Description**: Type the host pool's description.

> **Note:** Optionally, select **Generate using AI** to have AI create the description. See Overview of AI-Powered Description Generation for details.

- **Resource Group**: From the drop-down list, select the resource group for the host pool.
- **Desktop Experience**: From the drop-down list, select the desktop experience.

Note:

- **Multi user desktop (pooled)**: This is the full desktop experience. Users are not assigned to individual session hosts and are placed on a host based on its load. Multiple users are pooled together on a group of hosts.
- **Multi user RemoteApp (pooled)**: This is only published applications, not a full desktop experience. Published RemoteApps are visible to users as native apps running on their local computer. The RemoteApps are provided by a collection (pool) of session hosts.
- **Single user desktop (pooled)**: This is the full desktop experience. Users are placed on individual desktop VMs (one user per session host) and a preconfigured number of spare(available) desktops is maintained.
- **Single user desktop (personal)**: This is a personal (persistent) full desktop experience. A dedicated session host VM is assigned to each user.

- **Directory**: From the drop-down list, select the directory.

Note: The default option is the global default Nerdio Manager AD configuration. To use a custom configuration for the host pool, select the **Custom** option.

- **FSLogix**: From the drop-down list, select the FSLogix configuration profile to be used when creating or re-imaging hosts in this host pool.
- **RDP Profile**: From the drop-down list, select the RDP profile.
- **Name**: Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
    - **Prefix/Pattern**: From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
- **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
  - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
  - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).

- **Network**: From the drop-down list, select the network. The network determines the Azure region of the VM.

Note: Nerdio Manager verifies that there is a sufficient number of available IP addresses on the selected network before deploying new host pool VMs. If there are insufficient available IP addresses, an error message is displayed and you may not add the new host pool.

- **Desktop Image**: From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.
- **VM Size**: From the drop-down, select the VM disk size and type for newly created session hosts.

> **Note:** If any VM size is not available for a subscription or region, it doesn't appear in the list. At times, even if a VM size is available in a specific Azure region, it cannot be used due to the subscription having restrictions on a particular size. In such cases, we show the VM size in the drop-down list, but don't allow users to select it (the size is disabled).

- **OS Disk**: From the drop-down list, select the OS Disk type and size for newly created session hosts.

> **Note:** This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S- type) is not recommended. Premium SSD provides best performance.

- **Resource Group**: From the drop-down list, select the resource group to contain the VMs.
- **Quick Assign**: From the drop-down list, select the users or groups to pre-assign to newly created desktops.

> **Note:** The number of users specified cannot exceed the number of hosts being added. User assignment can be modified after the host pool is created.

- **Apply tags**: Optionally, type the **Name** and **Value** of the Azure tag to apply to the host pool.

> **Note:** You may specify multiple tags. See this Microsoft article for details about using tags to organize your Azure resources.

    - **Add "cm-resource-parent" tag**: Select this option to add the "cm-resource-parent" tag to the host pool.
- **App group settings**: Optionally, type the **App group name** of the host pool.

- **Application policies**: Optionally, select the application policies to assign to the host pool.
- **Validation environment**: Select this option to receive service updates at a faster cadence than non-validation host pools, allowing you to test service changes before they are deployed broadly to production.

6. Once you have entered all the desired information, select **OK**.
7. The auto-scale configuration window displays. If desired, configure the auto-scaling for the host pool. See "Enable Dynamic Host Pool Auto-scaling" on page 86 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" on page 86

"Host Pools" on page 76

Manage Auto-scale Profiles

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.

This feature is only available in the Nerdio Manager **Premium** edition.

Auto-scale profiles simplify the creation process for new host pools by allowing you to create a profile with auto-scale settings that can be reused. When configuring auto-scale for a host pool, you can select an auto-scale profile for both the standard and alternative auto-scale schedules.

This eliminates the need for manual configuration of the auto-scale settings for each pool or schedule.

To create an auto-scale profile:

1. Navigate to **Settings** > **Auto-scale profiles**.
2. Select **Add auto-scale profile**.
3. Enter the following information:
    - **Auto-scale mode**: From the drop-down list, select the auto-scale mode.

      Note: 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**: Type the profile name.
    - **Description**: Type the profile description.
    - For all the other parameters, see the relevant article:
        - For pooled dynamic host pools: "Enable Dynamic Host Pool Auto-scaling" on page 86
        - For single user desktop personal host pools: "Enable Personal Host Pool Auto-scaling" on page 99
4. Once you have entered all the desired information, select **Save**.

To assign auto-scale profiles to host pools:

1. Navigate to **Settings** > **Auto-scale profiles**.
2. Locate the auto-scale profile you wish to work with.
3. From the action menu, select **Assignments**.
4. Select **Add assignments**.
5. Enter the following information:
    - **Auto-scale profile**: From the drop-down list, select the auto-scale profile.
    - **Host pools**: From the drop-down list, select the host pool(s).
    - **Type**: From the drop-down list, select the assignment type- **Default** or **Alternative**.
    - **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.
    - **Schedule**: For Alternative profiles, optionally, toggle this option **On** and configure the schedule.
6. Once you have entered all the desired information, select **Save**.

Note: You may 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.

To manage auto-scale profiles:

1. Navigate to **Settings** > **Auto-scale profiles**.
2. Locate the auto-scale profile you wish to work with.
3. From the action menu, select any of the following options:
    - **Edit**: Edit the profile.
    - **Delete**: Delete the profile.
    - **Clone**: Clone the profile.

Enable Dynamic Host Pool Auto-scaling

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

The auto-scale feature ensures that only the number of session host VMs required to serve the current demand are running. When not in use, VMs are stopped or deleted. When demand rises, or at specific times of the day, additional VMs in the host pool are started or created. This allows for cost savings.

You can enable and configure the auto-scaling feature for dynamic host pools.

Note: By default, the **Auto-scale** option is disabled. When you enable auto-scaling, you can configure the desktop image, VM size, and OS disk template, and also set the criteria for host pool sizing, scaling logic, and pre-stage hosts.

To enable dynamic host pool auto-scaling:

1. Locate the dynamic host pool you wish to work with.
2. From the action menu, select **Auto-scale** > **Configure**.
3. Enter the following basic auto-scale information:
    - **Auto-Scale**: Toggle this option **On**.
    - **Auto-scale Timezone**: From the drop-down list, select the time zone for the auto-scale process.
    - **Name**: Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
        - **Prefix/Pattern**: From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
- **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
  - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
  - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).

- **Network**: From the drop-down list, select the network the VM connects to.

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

- **Desktop Image**: From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **VM Size**: From the drop-down list, select the VM size for new session hosts.
- **Running OS Disk (Template)**: From the drop-down list, select the OS disk type and size for new session hosts.
- **Stopped OS Disk Type**: From the drop-down list, select the OS disk type when session host VMs are stopped.

> **Note:** See Auto-Scale Cost Optimization OS Disk Storage for more information about OS disk auto-scale configuration.

- **Resource Group**: From the drop-down list, select the resource group where VMs should be created.
- **VM Naming**: From the drop-down list, select the VM naming to use.

> **Note:** Host VMs that are created automatically by the scale out or auto-grow process use names based on the selected VM naming mode. See How Session Host VM Names are Generated for more information.
>
> - **Re-use names**: Always attempt to re-use names that were previously used in the pool, if available.
> - **Standard names**: Use the next available name.
> - **Unique names**: Always attempt to use a unique name for new hosts.

- **Automatically Re-image Used Hosts**: Selecting this option to re-image hosts that had at least one user logged into them. For multi-session hosts, the hosts are re-imaged once the last user signs out.

4. Select the **Default schedule** or **Alternative schedule**.

> **Note:** Nerdio Manager allows you to configure separate auto-scale settings for a default schedule (normal operations) and an alternative schedule (outside of normal operations). For example, you may want fewer session hosts available on weekends or bank holidays. Alternatively, you may want more session hosts available two weeks prior to Christmas when you have a large number of temporary customer support agents. In either case, you would use the **Alternative schedule** tab to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, navigate to the **Alternative schedule** tab and enter the following information:

> **Note:** The Estimated Monthly Costs shown at the top of this page only consider the Default Schedule's settings.

  - **Schedule**: Toggle on the Schedule option to turn on the Alternative Schedule process.
  - **Days**: From the drop-down list, select the off-peak day(s).
  - **Dates**: Select the specific off-peak date(s).
  - Select **+** or **-** to add or remove off-peak dates.

5. Select the **Auto-scale profile (Premium only)**:
   - From the drop-down list, select the auto-scale profile to use. Alternatively, select **Custom** to create a custom auto-scale configuration.

> **Note:** See "Manage Auto-scale Profiles" on page 83 for details about creating and working with auto-scale profiles.

6. Enter the following **Host Pool Properties** information:
   - **Session limit host**: Type the maximum number of sessions per host. Once this session limit is reached, and there are no more available hosts, a new host is started automatically, if it exists.
   - **Load Balancing**: From the drop-down list, select the desired load balancing.

> **Note:**
>
> - **Breadth First** means that the load-balancing algorithm spreads the users evenly across all available session hosts.
> - **Depth First** means the load-balancing algorithm places all the users in the first session host until the host's session limit is reached. Only then, does it place the users in the next session host. If necessary, it powers on the VM and makes it available to the users.

- **Start on connect**: Select this option to start the session host VMs on connect.

7. Enter the following **Host Pool Sizing** information:

- **Active Host Defined As**: From the drop-down list, select the active host definition.

> **Note:** When set to “VM started,” the system identifies a session host VM as active as long as the VM is running in Azure. There are very few instances when "VM started" should be selected.
>
> When set to “AVD Agent Available,” the system identifies a session host VM as active only when the AVD back-end is receiving heartbeats and sees the session host as “Available.” In general, you should select "AVD Agent Available.”

- **Base Host Pool Capacity**: Type the number of session host VMs to always be part of this host pool. These session hosts may be stopped or running.
- **Min Active Host Capacity**: Type the minimum number of running session hosts that are always available. Typically, a session host must be running for users to sign in or the "Start on connect" feature is enabled. Other VMs can be either stopped or turned on, as configured by the user auto-scaling logic.
- **Burst Beyond Base Capacity**: Type the capacity to burst above the standard number of session host VMs when there is user demand. The system automatically creates up to this number of new session host VMs above the **Base Host Pool**

Capacity, when needed. These session hosts are the first ones to be removed when the system scales in after business hours.

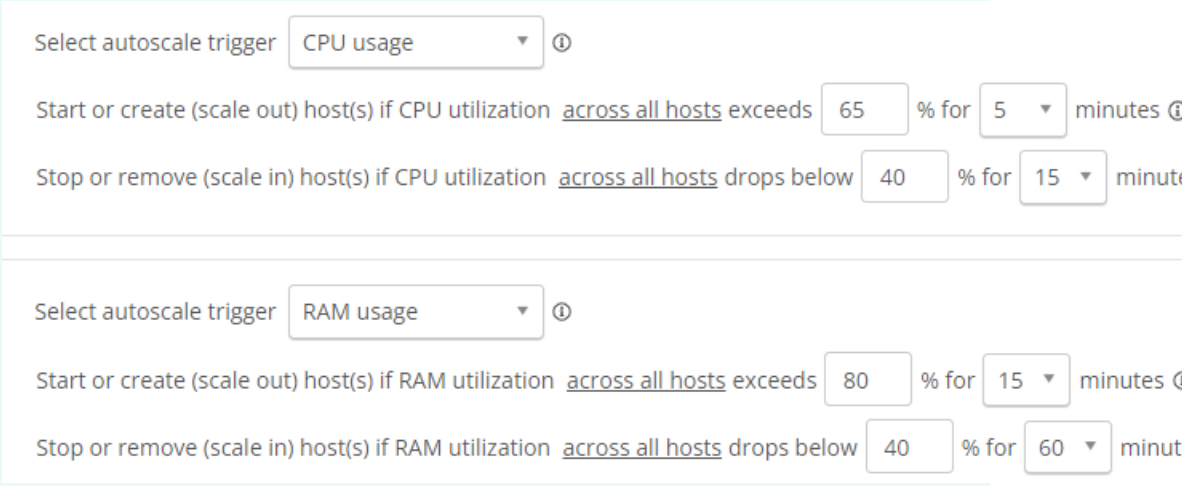
8. Enter the following **Scaling Logic** information:

   - **Use Multiple Auto-scale Triggers**: Select this option to enable multiple usage triggers to be used for scaling out and scaling in.

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

     Notes:

     - Auto-scale adds capacity when **any** of the scale out conditions are met. Capacity is removed only when **all** the scale in conditions are met.
     - Use the + and - buttons to add or remove scale out triggers. You may select up to 3 triggers.

   - **Select Auto-scale Trigger**: From the drop-down list, select the auto-scale trigger.

Note: The available triggers are:

- **CPU usage** or **RAM usage**: This scales out when the average CPU or RAM usage across all running session hosts in the pool exceeds a predefined value for a predefined duration.
- **Average active sessions**: This scales out when the average number of active sessions per host exceeds a predefined value.
- **Available sessions**: This maintains the number of available hosts by scaling out and scaling in within the limits of the Host Pool Sizing and the maximum number of sessions per host.
- **User-driven**: Hosts are started when users connect and are automatically stopped after a defined amount of time after all users sign out.

- For **CPU usage or RAM usage**:
  - **Start or Create (Scale Out) Up To**: Scale out by starting (if there are stopped VMs) or creating (if there are no stopped VMs) session hosts if the trigger is exceeded.
  - **Stop or Remove (Scale In) Up To**: Scale in by stopping (if there are no burst VMs) or removing (if there are burst VMs) session hosts if scale in trigger is met.
- For **Average active sessions**:
  - **Start or Create (Scale Out) Up To**: Scale out by starting (if there are stopped VMs) or creating (if there are no stopped VMs) session hosts if the average active sessions across all hosts is exceeded.
  - **Stop or Remove (Scale In) Up To**: Scale in by stopping (if there are no burst VMs) or removing (if there are burst VMs) session hosts if if the average active sessions across all hosts is below the number specified.
- For **Available sessions**:

- **Maximum sessions per host**: Type the maximum sessions per host.
- **Maintain up to X available sessions**: Type the number of sessions that must be available either always or during work hours.

> **Note:** This ensures that there are this many available sessions during work hours or at all times. Work hours start at **Start of work hours** specified in the **Pre-Stage Hosts** section and end at the beginning of scale in period specified in the Scale in restrictions section below.

  - **Outside work hours**: Type the number of sessions to maintain outside of work hours.

> **Note:** This value cannot exceed the number of desktops available during work hours.

  - **Working hours**: From the drop-down lists, select the start and end times for working hours.

- For **User Driven**:
  - **When all users log off, scale in hosts after**: From the drop-down list, select the number of minutes to scale in after all users have signed out.

> **Note:** Desktops are automatically stopped only when there are no active or disconnected sessions. To automatically sign out disconnected users after a certain time, use the user session limits settings on the host pool properties.

- **Scale in Restrictions**:
  - **Stop or Remove (Scale In) Hosts Only From**: From the drop-down list, select the time to perform the scale in operation. Select **<any time>** to allow scaling in to be performed at any time.

- **Scale In Aggressiveness**: From the drop-down list, select the scale in aggressiveness.

  Note:

  - **High Aggressiveness**: Scale in aggressiveness is set to **High** by default, which means it is guaranteed that after business hours, hosts that have active or disconnected sessions running on them are automatically deleted or powered off to reduce capacity. After business hours, the auto-scale logic first removes the hosts that have no sessions running on them. The remaining hosts are sorted based on the least number of sessions running on them. The users with active sessions are then consolidated and moved to a single host and the other hosts are removed by auto-scale. A warning message is sent to the active session users before removing the session hosts.
  - **Medium Aggressiveness**: When scale in aggressiveness is set to **Medium**, after business hours, the scaling logic only removes the hosts that have disconnected sessions running on them. The session hosts with active sessions running on them won't be removed. In this case, the host pool is scaled in to some extent.
  - **Low Aggressiveness**: When scale in aggressiveness is set to **Low**, after business hours, the scaling logic only removes those session hosts that have absolutely no sessions running on them. The auto-scale logic does not remove any session host that have sessions, either active or disconnected, running on them. Though this option is less disruptive for the users, there is no guarantee that the host pool is ever scaled in.

- **Deactivate (drain mode) hosts**: Optionally, you can tell the auto-scale engine to deactivate all hosts at the start of the scale in window. It does leave the minimum number of hosts as specified in the **Min active host capacity** in the **Host Pooling Size** section.

9. Enter the following **Rolling Drain Mode** information:

Notes:

- You can create multiple drain windows and target a specific percentage of your hosts to drain mode, outside of the Scale-in Restriction window. This feature allows you to prevent new connections to a percentage of hosts and allows these hosts to be shut down more quickly, saving on resource costs.
- Rolling drain mode selects hosts to scale in as follows:
  - First, it starts with lowest active sessions.
  - Then it scales in hosts that are already in drain mode,
  - Finally, it scales in hosts with the lowest number of total sessions (active + disconnected).

- **Rolling Drain Mode**: Toggle this option on to enable rolling drain mode.
- **Window name**: Type the name for this drain window.
- **Start time**: From the drop-down lists, select the start time when this drain window comes into effect.

  Note: The last drain window remains in effect until 11:59 PM.

- **% hosts in drain mode**: Type the percentage of hosts in drain mode during this window.

  Note: Use − + to add or remove drain windows.

- **Load balancing**: From the drop-down list, select the preferred load balancing algorithm.

Note: This option is only available in the Nerdio Manager **Premium** edition.

- **Depth First**: The load balancing algorithm places users on a single host until the session limit is reached, at which point users start being placed on the next host until the session limit is reached again.
- **Breadth First**: The load balancing algorithm spreads users evenly across available session hosts.

- **Scale in aggressiveness**: From the drop-down list, select the scale in aggressiveness.

Note: See the details in the **Scale in Restrictions** section above.

10. Enter the following **Pre-Stage Hosts** information:

Note: Configure the system to automatically pre-stage some hosts as available capacity with respect to the business hours. For example, you can pre-stage hosts at the beginning of the work day, so the system does not have to auto-scale in real time for users who all sign in at the same time when they start work.

- **Use Multiple Schedules**: Select this option to enable multiple, non-overlapping pre-staging schedules to be used.

Note: This is not available for the Available Sessions trigger when During Work Hours option is specified.

- **Work Days**: From the drop-down list, select the work days when pre-stage tasks should be run.
- **Start of Work Hours**: From the drop-down select the starting hour when pre-stage tasks should be run.

- **Host to be Active by Start of Work Hours**: Type the number of session hosts that should be ready to accept user connections by this time.
- **Scale In Delay**: From the drop-down list, select a delay to restrict scale in operations after the start of work hours. Pre-staged hosts are not scaled in during this time even if they are unused.

11. Enter the following **Messaging** information:

> **Note:** The system sends messages to any users connected to a session host that has been selected for scale in.

- **Send a Warning Message to Users on the host**: From the drop-down list, select the number of minutes before scaling in that the message should be sent.
- **The message should say**: Type the warning message text.

12. Enter the following **Auto-Heal Broken Hosts** information:

> **Note:** Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts**: Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is**: From the drop-down lists, select the desired statuses along with the sessions status.

> **Note:** The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft article for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

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

> **Notes:**
>
> - You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
> - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.

- **Minutes between recovery actions**: Type the number of minutes to wait after each restart attempt before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

> **Note:** If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

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

Related Topics

"Create Dynamic Host Pools" on page 78

"Enable Personal Host Pool Auto-scaling" on the next page

Enable Personal Host Pool Auto-scaling

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

Nerdio Manager allows you to perform auto-scaling on personal host pools. This enables you to do the following:

- Personal desktops can be automatically powered on and off based on a schedule. Alternatively, personal desktops can be stopped when there are no active or disconnected sessions.
- The host OS disk type can be changed to a lower priced storage type when the personal desktop is not running.
- Auto-healing automatically attempts to repair "broken" session hosts. In addition, it allows scripted actions, such as SxS re-install or AVD host re-register, to be executed against them.

To configure the basic auto-scale information:

1. Locate the personal host pool you wish to work with.
2. From the action menu, select **Auto-scale** > **Configure**.
3. **Auto-Scale**: Toggle this option **On**.
4. Enter the following basic auto-scale information:
    - **Auto-scale Timezone**: From the drop-down list, select the time zone for the auto-scale process.
    - **Name**: Type the name of the newly added hosts for Prefix or the Prefix+Pattern.
        - **Prefix/Pattern**: From the drop-down list, select whether to use a Prefix or a Pattern.

Note:

- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
- **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
  - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
  - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).

- **Network**: From the drop-down list, select the network the VM connects to.

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

- **Desktop Image**: From the drop-down list, select a desktop image to be used as the golden image for new session hosts.
- **VM Size**: From the drop-down list, select the VM size for new session hosts.
- **Running OS Disk (Template)**: From the drop-down list, select the OS disk type and size for new session hosts.
- **Stopped OS Disk Type**: From the drop-down list, select the OS disk type when session host VMs are stopped.

- **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.).

- **Resource Group**: From the drop-down list, select the resource group where VMs should be created.
- **VM Naming**: From the drop-down list, select the VM naming to use.

Note: Host VMs that are created automatically by the scale out or auto-grow process use names based on the selected VM naming mode. See How Session Host VM Names are Generated for more information.

- **Re-use names**: Always attempt to re-use names that were previously used in the pool, if available.
- **Standard names**: Use the next available name.
- **Unique names**: Always attempt to use a unique name for new hosts.

5. Select the **Default schedule** or **Alternative schedule**.

Note: Nerdio Manager allows you to configure separate auto-scale settings for a default schedule (normal operations) and an alternative schedule (outside of normal operations). For example, you may want fewer session hosts available on weekends or bank holidays. Alternatively, you may want more session hosts available two weeks prior to Christmas when you have a large number of temporary customer support agents. In either case, you would use the **Alternative schedule** tab to configure the auto-scale settings for those periods that are outside of normal operations.

- To create an alternative schedule, navigate to the **Alternative schedule** tab and enter the following information:

Note: The Estimated Monthly Costs shown at the top of this page only consider the Default Schedule's settings.

- **Schedule**: Toggle on the Schedule option to turn on the Alternative Schedule process.
- **Days**: From the drop-down list, select the off-peak day(s).

- **Dates**: Select the specific off-peak date(s).
- Select **+** or **-** to add or remove off-peak dates.

6. **Auto-scale Mode**: From the drop-down list, select the desired auto-scale mode.

> **Notes:**
>
> - **User- driven**: The auto- scaling is performed when there are no active or disconnected sessions.
> - **Schedule-based**: The auto-scaling is performed as per the specified schedule.

7. **Auto-scale profile (Premium only)**: Optionally, from the drop-down list, select the auto-scale profile to use. Alternatively, select **Custom** to create a custom auto- scale configuration.

> **Note:** See "Manage Auto-scale Profiles" on page 83 for details about creating and working with auto-scale profiles.

8. Continue the configuration process with the relevant auto-scale mode:
   - **User-driven**: See "To enable user-driven personal host pool auto-scaling:" below
   - **Schedule-based**: "To enable schedule-based personal host pool auto-scaling:" on page 110

To enable user-driven personal host pool auto-scaling:

1. **Auto-scale Mode**: From the drop-down list, select the **User-driven**.
2. Enter the following **Host Pool Properties** information:
   - **Start on connect**: Select this option to start the desktop on connect.
3. Enter the following **Desktop Start and Stop** information:

- **Desktop Start and Stop**: Toggle this option on to enable desktop start and stop.
- **Desktops are stopped when users log off after**: From the drop-down list, select the number of minutes or hours to scale in after all users have signed out.

> **Notes:**
>
> - Desktops are automatically started when users connect.
> - Desktops are automatically stopped only when there are no active or disconnected sessions. To automatically sign out disconnected users after a certain time, use the user session limits settings on the host pool properties.

- **Bypass drain mode for desktops in this pool**: Select this option so that desktops do not enter drain mode before shutdown.

4. Enter the following **Pre-stage Host OS Disks** information:

- **Pre-stage Host OS Disks**: Toggle this option on to enable pre-staging OS disks.
- From the drop-down lists, select the **Days** and **Times** the session host VMs' OS disks should be pre-staged.
- **Leave desktops that are not assigned to a user with STOPPED OS disk type**: Select this option so that desktop VMs that are unassigned to a user do not have the OS disk converted from STOPPED to RUNNING.
- **Use intelligent disk pre-staging for users**: Select this option to have intelligent disk pre-staging learn user behavior and automatically adjusts the disk pre-stage times.

> **Note:** This feature requires AVD insights to be enabled and configured for the host pool.

- **Mode**: From the drop-down list, select the mode.

> **Note:**
>
> - **Hybrid Mode**: Disks are always be pre-staged based on the defined schedule. The behavior of users whose work patterns are learned, and additional staging activity are scheduled. This function is designed as "learning mode," with the benefits of both the standard pre-stage functionality and learned requirements.
> - **Automated Mode**: Disks are pre-staged for existing users only according to the learned schedule. New users respect the defined schedule until Intelligent pre-staging has enough data to automate this process. Disks are pre-staged 30 minutes before anticipated user log on events.

5. Enter the following **Auto-Grow** information:

> **Note:** Automatically add desktops to the host pool when the number of unassigned desktops remaining falls below a specified threshold.

- **Auto-Grow**: Toggle this option on to enable auto-grow.
- **Add a new host when the number of available (not assigned to a user) falls below**: Type the threshold and from the drop-down list, select whether the threshold is a number of desktops or a percentage of total desktops.

6. Enter the following **Auto-Shrink** information:

> **Note:** The system automatically remove desktops that have not been used in a long time.

- **Auto-Shrink**: Toggle this option on to enable auto-shrink.
- **Delete VM if the user hasn't logged in for**: Type the number of days to wait before the system automatically deletes the VM.

> **Note:** User activity on this session host VM is determined based on Nerdio Manager auto-scale history and AVD diagnostics data. Each time the desktop is processed by auto-scale, an Azure tag with date/time the desktop was last used is set. If the desktop hasn't been used for the number of days specified in this setting, the session host VM is shut down and a "pending deletion" tag is set.

- **Desktop will be set to "Pending deletion" state and deleted after**: From the drop-down list, select the "Pending deletion" duration.

> **Note:** The desktop is set to "Pending deletion" state by the auto-scale process by adding a tag to the VM. A task is logged during this process, which can be used for admin notification of a desktop entering the "Pending deletion" state. There also are notification banners in the Nerdio Manager UI indicating that a personal host pool has VMs that are pending deletion. After the "pending deletion" period expires (default: 24 hours), the VM is permanently deleted.

- **Exclude the following groups (or individual users)**: Enable this option, and then select the group(s) or individual user(s) to exclude from auto-shrink.

> **Note:** Desktops assigned to users listed here are **not** automatically removed, even after a prolonged time of inactivity.

- **Exclude unassigned Desktops from Auto-shrink**: Select this option to exclude desktops that have not been assigned to a user from the auto-shrink operations.

> **Note:** Use this setting in combination with Auto-Grow to maintain a buffer of free unassigned desktops.

- **Scripted actions to run when a host is scheduled to shrink**: From the drop-down list, select the scripted action(s) to run after the VM is marked to auto-shrink.
- **Notify users of scheduled deletion**: Select this option to notify the user via email about deletion of their desktop when the inactivity period is exceeded.

> **Note:** Notifications on the **Settings** > **Nerdio environment** page must be enabled for this feature to work.

  - **Message Subject**: Expand this option to type the subject line of the auto-shrink message.
  - **Message Text**: Expand this option to open the editor to create a custom auto-shrink message for users.

Note: The following variables are available for use in the message body:

- **%HOSTPOOL%**: Returns the name of the affected host pool.
- **%HOSTNAME%**: Returns the specific host name.
- **%HOST_ IDLE_ DAYS_ THRESHOLD%**: Returns the configured maximum idle days before auto shrink is started.
- **%SHRINK_TIME_UTC%**: Returns the exact time in UTC when the auto-shrink task is set to occur.
- **%SHRINK_DATE%**: Returns the exact date when the auto-shrink task is set to occur.
- **%SHRINK_DATE_EUR%**: Returns the exact date when the auto-shrink task is set to occur in dd/MM/YYYY (European) format.
- **%IMAGE_NAME%**: Returns the VM's image name.
- **%FRIENDLY_ WORKSPACE_ NAME%**: Returns the workspace's friendly name.
- **%FRIENDLY_ HOSTPOOL_ NAME%**: Returns the host pool's friendly name.
- **%VM_SIZE%**: Returns the VM's size.
- **%DISK_SKU%**: Returns the VM's disk SKU.
- **%USER_NAME%**: Returns the name of the user logged in to the VM.

- **Notify an additional email recipient when desktops are scheduled to be deleted**: Select this option to notify an additional email recipient when desktops are scheduled to be deleted.
  - **Send notification emails to**: Type the additional recipient's email address.
  - **Send notification emails from**: Type the sender's email address.

- **Notifications frequency (Premium only)**: From the drop-down list, select how frequently the email reminders are sent to the user.

> **Note:** A final email is always be sent 1 day before the scheduled deletion.

7. Enter the following **Auto-Heal Broken Hosts** information:

> **Note:** Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts**: Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is**: From the drop-down lists, select the desired statuses along with the session status.

> **Note:** The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft article for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

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

> **Notes:**
>
> - You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
> - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.

- **Minutes between recovery actions**: Type the number of minutes to wait after each recovery action step before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

> **Note:** If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

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

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

1. **Auto-scale Mode**: From the drop-down list, select the **Schedule-based**.
2. Enter the following **Host Pool Properties** information:
    - **Start on connect**: Select this option to start the desktop on connect.
3. Enter the following **Working Hours** information:
    - From the drop-down lists, select the **Days** and **Times** the session host VMs' OS disks should be pre-staged.
    - **Power off aggressiveness**: From the drop-down list, select the power off aggressiveness. (Schedule-based only)

Note:

- **High**: Power off all session host VMs, including those with active and disconnected sessions. Users with active sessions are sent a message, defined below, and given time to sign out before their session host VM is powered off.
- **Medium**: Power off only those session host VMs that do not have an active user session, including those with disconnected sessions.
- **Low**: Only power off those session host VMs that have no active or disconnected sessions.

- **Power on timing**: From the drop-down list, select the power on timing. (Schedule-based only)

Note:

- **Never**: Do not power on session host VMs at the beginning of the working hours defined above. Users must manually power on their session host VMs.
- **Once**: All sessions host VMs are only powered on once at the start of the working hours. If a session host VM is powered off after the start of the working hours, it is not automatically powered back on by auto-scale.
- **Continuously**: All session host VMs are powered on at the start of the working hours. In addition, for the duration of the working hours, auto-scale automatically powers on any session host VMs that were manually powered off.

- **Power off timing**: From the drop-down list, select the power off timing.

Note:

- **Never**: Do not power off session host VMs at the end of the working hours defined above.
- **Once**: At the end of the working hours, all session host VMs are powered off, subject to the aggressiveness defined above. If any session host VMs are manually powered on outside of the working hours, auto-scale does not automatically power them off.
- **Continuously**: At the end of the working hours, all session host VMs are powered off, subject to the aggressiveness defined above. If any session host VMs are manually powered on outside of the working hours, auto-scale automatically powers them off, subject to the aggressiveness defined above.

- **Include hosts without assigned user**: Select this option to also start unassigned desktops during the auto-scale process.

Note: This may be useful for organizations wishing to perform scheduled tasks against desktops during the working day.

4. Enter the following **Host OS Disks** information:

- **Set all hosts to running OS disk type during work hours**: Select this option to convert all stopped host VM OS disks to running disk type during the working hours defined above.

Note: This is necessary to ensure that if a VM is started via Azure Start VM on Connect that it has the correct, high-performance disk type. When this setting is enabled, all "Disk type differs from policy" warnings are hidden for this pool.

- **Use intelligent disk pre-staging for users**: Select this option to have intelligent disk pre-staging learn user behavior and automatically adjusts the disk pre-stage times.

> **Note:** This feature requires AVD insights to be enabled and configured for the host pool.

  - **Mode**: From the drop-down list, select the mode.

> **Note:**
>
> - **Hybrid Mode**: Disks are always be pre-staged based on the defined schedule. The behavior of users whose work patterns are learned, and additional staging activity are scheduled. This function is designed as "learning mode," with the benefits of both the standard pre-stage functionality and learned requirements.
> - **Automated Mode**: Disks are pre-staged for existing users only according to the learned schedule. New users respect the defined schedule until Intelligent pre-staging has enough data to automate this process. Disks are pre-staged 30 minutes before anticipated user log on events.

5. Enter the following **Auto-Grow** information:

> **Note:** Automatically add desktops to the host pool when the number of unassigned desktops remaining falls below a specified threshold.

   - **Auto-Grow**: Toggle this option on to enable auto-grow.
   - **Add a new host when the number of available (not assigned to a user) falls below**: Type the threshold and from the drop-down list, select whether the threshold is a number of desktops or a percentage of total desktops.

6. Enter the following **Auto-Shrink** information:

Note: The system automatically remove desktops that have not been used in a long time.

- **Auto-Shrink**: Toggle this option on to enable auto-shrink.
- **Delete VM if the user hasn't logged in for**: Type the number of days to wait before the system automatically deletes the VM.

  Note: User activity on this session host VM is determined based on Nerdio Manager auto-scale history and AVD diagnostics data. Each time the desktop is processed by auto-scale, an Azure tag with date/time the desktop was last used is set. If the desktop hasn't been used for the number of days specified in this setting, the session host VM is shut down and a "pending deletion" tag is set.

- **Desktop will be set to “Pending deletion” state and deleted after**: From the drop-down list, select the "Pending deletion" duration.

  Note: The desktop is set to "Pending deletion" state by the auto-scale process by adding a tag to the VM. A task is logged during this process, which can be used for admin notification of a desktop entering the "Pending deletion" state. There also are notification banners in the Nerdio Manager UI indicating that a personal host pool has VMs that are pending deletion. After the "pending deletion" period expires (default: 24 hours), the VM is permanently deleted.

- **Exclude the following groups (or individual users)**: Enable this option, and then select the group(s) or individual user(s) to exclude from auto-shrink.

  Note: Desktops assigned to users listed here are **not** automatically removed, even after a prolonged time of inactivity.

- **Notify user when their desktop is about to be deleted**: Select this option to notify the user via email about deletion of their desktop when the inactivity period is

exceeded.

> **Note:** Notifications on the **Settings** > **Nerdio environment** page must be enabled for this feature to work.

- **Message Subject**: Expand this option to type the subject line of the auto-shrink message.
- **Message Text**: Expand this option to open the editor to create a custom auto-shrink message for users.

  > **Note:** The following variables are available for use in the message body:
  >
  > - **%HOSTPOOL%**: Returns the name of the affected host pool.
  > - **%HOSTNAME%**: Returns the specific host name.
  > - **%HOST_ IDLE_ DAYS_ THRESHOLD%**: Returns the configured maximum idle days before auto shrink is started.
  > - **%SHRINK_TIME_UTC%**: Returns the exact time in UTC when the auto-shrink task is set to occur.
  > - **%SHRINK_DATE%**: Returns the exact date when the auto-shrink task is set to occur.

- **Notify an additional email recipient when desktops are scheduled to be deleted**: Select this option to notify additional users about auto-shrink activity.
  - **Send notification emails to**: Type the additional email addresses.
- **Send notification emails from**: From the drop-down list, select the "Send From" email address.

7. Enter the following **Messaging** information:

Note: The system sends messages to any users connected to a session host that has been selected for scale in.

- **Send a warning message to active users**: From the drop-down list, select the number of minutes before scaling in that the message should be sent.
- **The message should say**: Type the warning message text.

8. Enter the following **Auto-Heal Broken Hosts** information:

Note: Session hosts may get impaired due to domain trust issues or FSLogix configuration issues. The AVD agent reports the status of such hosts as unavailable. Admins then have to manually remove such hosts from the pool. However, Nerdio Manager allows you to configure a set of actions to repair these session hosts during the auto-scale process. Auto-scale can automatically attempt to repair "broken" session hosts by restarting and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into an operational state and then either leave it alone or delete and recreate the host.

- **Auto-Heal Broken Hosts**: Toggle this option on to enable auto-heal.
- **Host is Broken if AVD Agent Status is**: From the drop-down lists, select the desired statuses along with the session status.

Note: The status is reported to the AVD service by the AVD agent installed on the session host VM. If something is wrong, the status is something other than "Available." Not every status other than "Available" means that there is a problem. See this Microsoft article for more details. Hosts with active sessions may still be somewhat functional and such hosts are not treated as broken. Only hosts that have either no sessions at all or no active session (that is, disconnected sessions only) are considered broken by auto-scale.

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

> **Notes:**
>
> - You may select a VM action (for example, Restart VM or Remove VM), or a scripted action (for example, reinstall SxS, re-register host with AVD, etc.).
> - The recovery actions are run in the order shown. You can drag and drop any action to change its place in the list and, therefore, the order it is run.

- **Minutes between recovery actions**: Type the number of minutes to wait after each recovery action step before moving on to next step (for example, Restart VM, then Remove VM, then etc.).

> **Note:** If the Auto-Heal operation requires deletion and re-creation of a broken host VM, a spare VM is powered on to replace the capacity, if available.

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

Related Topics

"Create Dynamic Host Pools" on page 78

"Enable Dynamic Host Pool Auto-scaling" on page 86

Auto-scale: Cost Optimization Session Host VM OS Disk Storage

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.

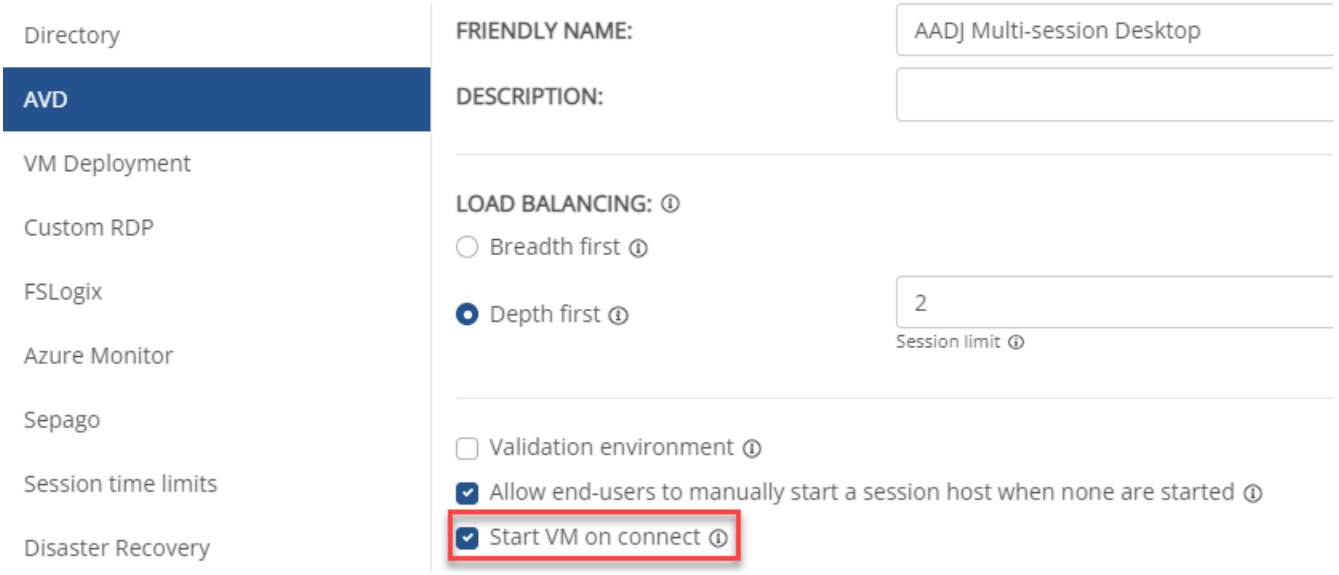
There are two types of costs associated with a VM - compute costs and storage costs. Compute costs are incurred only when the VM is in use, while the storage costs are incurred even when the VM is stopped.

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 **Workspaces** > **Dynamic host pools**.
2. Locate the single-user host pool you wish to change.
3. From the action menu, select **Auto-scale**> **Configure**.
4. In the **Host OS Disks** section, configure the following:

- **Running**: From the drop-down list, select the disk type when the VM is running.
- **Stopped**: From the drop-down list, select the disk type when the VM is stopped.

5. Once you have changed the parameters above, select **`Save & close`**.

For a multi-user host pool that has its **Minimum Active Host Capacity** set to 0, you can configure the system so that all stopped VM OS disks are automatically converted to **Running OS Disk** type during the pre-staging hours. This is necessary to ensure that if a VM is started via **Azure Start VM on Connect** that it has the proper high-performance disk type.

To configure the pre-staging OS disk type conversion:

1. Locate the single-user host pool you wish to work with.
2. From the action menu, select **Auto-scale**> **Configure**.
3. In the **Pre-stage Hosts** section, configure the following:
   - If necessary, enable **Pre-stage hosts**.
   - **Set all host to running OS disk type**: Select this option.
   - Set the pre-stage time as desired.
4. Once you have entered all the desired information, select **`Save & close`**.

Add a New Session Host to a Dynamic Host Pool

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

Once a host pool is created, you can manually add session hosts.

Tip: When using Dynamic Host pools it is recommended that you create the hosts with auto-scaling configured. See "Enable Dynamic Host Pool Auto-scaling" on page 86 for more information.

To add a session host to a dynamic host pool:

1. Locate the dynamic host pool you wish to work with.
2. From action menu, select **Hosts** > **Add new**.
3. Enter the following information:

Note: For several of the required parameters, you may filter the available choices by using the Resource Selection Rules. For example, you may filter the VM Size or OS Disk choices for Intel RAM-optimized VMs only. See "Resource Selection Rules Management" on page 50 for details.

- **Run now** or **Schedule**: Optionally, navigate to the **Schedule** tab to perform the task during selected time frame(s). Otherwise, the task starts as soon as you select **Save**. See "Manage Schedules for Tasks" on page 46 for details about creating a schedule.
- **Host Count**: Type the number of session hosts to add to the host pool during creation.
- **Host Name**: Type the name of the newly added hosts for the Exact name, a Prefix or the Prefix+Pattern.
  - **Exact/Prefix/Pattern**: From the drop-down list, select whether to use an Exact name, a Prefix, or a Pattern.

Note:

- **Exact** applies when adding a single host and specifying an exact name. For example, MYADVHOST.
- **Prefix** can be used when creating multiple session hosts. The Prefix limit is 10 valid, Windows computer name characters. When using a Prefix, a unique suffix is automatically appended in the format "-xxxx", where xxxx are 4 random alphanumeric characters. For example: AVDHOST-s72h. Do not add a "-" to the Prefix.
- **Pattern** can be used to specify an advanced naming convention for new hosts. Pattern characters must be enclosed in {} and can be # (for sequential numbers) and/or ? (for random alphanumeric characters). One # implies numbers from 0 to 9, two #s implies numbers of 0 to 99, etc.
  - Example 1: AVDHOST{###} (AVDHOST000..AVDHOST999).
  - Example 2: AVDHOST-{???} (AVDHOST-d83, AVDHOST-7sl, etc.).

- **Network**: From the drop-down list, select the network. The network determines the Azure region of the VM.
- **Desktop Image**: From the drop-down list, select the desktop image that is used as the golden image for newly created session hosts.

Note: The **Unmanaged Azure Compute Gallery image versions** section is at the bottom of the list. These are unmanaged, backup versions of images that were created while activating staged images. These images can be used to restore any changes made to session hosts.

- **VM Size**: From the drop-down, select the VM type for newly created session hosts.
- **OS Disk**: From the drop-down list, select the OS Disk type and size for newly created session hosts.

> **Note:** This must be equal to or larger than the size of the Desktop Image selected above. Using Standard HDD (S-type) is not recommended. Premium SSD provides best performance.

- **Resource Group**: From the drop-down list, select the resource group to contain the VMs.
- **Apply tags**: Optionally, type the **Name** and **Value** of the Azure tag to apply to the session host.

> **Note:** You may specify multiple tags. See this Microsoft article for details about using tags to organize your Azure resources.

- When **Host Count** is greater than 1, enter the following:
  - **Process Host in Groups Of**: Type the number of concurrent operations when adding the new hosts.
  - **Number of failures before aborting**: Type the number of failed tasks before the process stops.
- **Schedule**: If scheduled, enter the schedule information to run this job per the schedule.

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

Host Pool AVD Configuration

> **Warning:** Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

Nerdio Manager enables you to customize the host pool's AVD settings.

To configure host pool AVD settings:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties** > **AVD**.
3. Enter the following information:.
    - **Friendly Name**: Type the friendly name that is visible to the end users.
    - **Description**: Type the description that is visible to the administrators.

      Note: Both the Friendly Name and Description can be changed at any time.

    - **Load Balancing**: Select the desired load balancing option.

      Note: The load balancing algorithm is used by the AVD Management Service to determine how to route a particular user's desktop or RemoteApp connection.

      Breadth First means that the load-balancing algorithm spreads the users evenly across all available session hosts.

      Depth First means the load-balancing algorithm places all the users in the first session host until the host's session limit is reached. Only then, does it place the users in the next session host. If necessary, it powers on the VM and makes it available to the users.

        - **Session Limit**: Type the number of sessions that a single host in the host pool can accept.
    - **Validation environment**: Select this option designate this host pool as a validation host pool.

      Note: Validation host pools receive service updates at a faster cadence than non-validation host pools, allowing you to test service changes before they are deployed broadly to production.

- **Allow the users to manually start a session host when none are started**: Select this option to allow a user to sign in to Nerdio Manager and perform service actions. For example, power on the session hosts within the host pool. Only specified users that have the permissions to sign in to Nerdio Manager can start the session host VM this way.
- **Start VM on connect**: The VM is powered on automatically when the user connects. Any user can start the VM when they sign in.
- **Unassign user from host pool when removing host**: For personal host pools, select this option to unassign the user from the host pool when the host is deleted.
- **Collect hosts CPU usage**: Select this option to have the auto-scale process always collect CPU usage regardless of the host pool's auto-scale trigger.
- **Collect hosts RAM usage**: Select this option to have the auto-scale process always collect RAM usage regardless of the host pool's auto-scale trigger.
- **Collect hosts average active sessions**: Select this option to have the auto-scale process always collect average active sessions data regardless of the host pool auto-scale trigger..
- **Enable Scheduled AVD Agent Update**: Toggle on this option to specify the day and time you want to update the AVD agent.

> **Note:** Deploying updates at convenient times, or outside of peak business hours, ensures greater reliability and business continuity, while also enhancing the employee experience without interrupting business critical work.

  - **Time Zone**: From the drop-down list, select the time zone for the scheduled update.

> **Note:** Setting the time zone ensures that updates to the session host VMs in the host pool take place at the same time according to the selected time zone, regardless of the session host VMs' local time zones. See this Microsoft article for details.

- **Use local session host time zone**: Select this option to perform the agent update using the local time zone of each session host VM in the host pool.

  > **Note:** . Use this setting when all session host VMs in your host pool, or their assigned users, are in different time zones.

- **Maintenance window**: From the drop-down lists, specify the day and time for the agent update.

  > **Note:** All maintenance windows are two hours long.

- **Set additional maintenance window**: Optionally, select this option to specify a second maintenance window.

  > **Note:** Creating two maintenance windows gives the agent components an additional opportunity to update if the first update is unsuccessful.

- **Power on all hosts during window(s)**: Optionally, select this option to power on all hosts in a pool during maintenance window operations to ensure the installation of the latest AVD agent and other updates.

  > **Note:** Hosts that are started as part of this process are shut down after 2 hours. Hosts that were already running do not have their power state changed.

- **Exclude Drain mode hosts**: Optionally, select this option to exclude drain mode hosts from the AVD agent maintenance window tasks configured in the host pool properties.

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

Host Pool VM Deployment

Warning: Nerdio Manager does not install the BgInfo Azure extension during any automation or management process. However, the BgInfo extension may be installed either through a scripted action directly, or unintentionally, as stated in the Azure PowerShell module issues report.

Nerdio Manager enables you to customize the way session host VMs are deployed in a host pool. This is a feature-rich facility that is detailed below.

To configure host pool VM deployment:

1. Locate the host pool you wish to work with.
2. From the action menu, select **Properties** > **VM Deployment**.
3. Enter the following information:.
    - **Set time zone**: Select this option, and from the drop-down list select the time zone, to set the time zone on the VM when it is provisioned.
    - **Enable time zone redirection**: Select this option to allow users to see their local device's time zone inside of their session.
    - **Enable Accelerated Networking for VMs that support it**: Select this option to enable Accelerated Networking, if available.

      Note: The Azure VM accelerated networking feature is available in some of the larger Azure VMs. This feature is useful for enterprise organizations and IT professionals who need to deploy, manage, and optimize large amounts of Azure Virtual Desktops. It speeds up networking performance of individual VMs.

      If this feature is not supported on your Azure VM, it is not enabled. See this Microsoft document for more information.

- **Enable NVMe for VMs that support it**: Select this option to enable NVMe, if available.

> **Note:** NVMe is a storage protocol that offers higher IOPs and throughput providing your workload with overall greater performance. See this Microsoft document for more information.

- **Install GPU drivers on supported VM sizes**: Select this option to install either NVidia or AMD drivers.

> **Note:** GPU drivers can be installed on N-series VMs.

- **Distribute VMs across Availability Zones**: Select this option to automatically distribute newly created or re-imaged session host VMs across Availability Zones in the selected Azure region.

> **Note:** See this Microsoft article for more details about Azure Regions and Availability Zones.

- **Place VMs on Dedicated Hosts**: Select this option to place the VMs to physical servers.

> **Note:** See this Microsoft article for more details about Azure dedicated hosts.

  - **Dedicated Host Group**: From the drop-down list, select the dedicated host group.
  - **Dedicated Host**: From the drop-down list, select the dedicated host for the VMs.

> **Note:** If **Automatic assignment** is selected, the VMs are automatically assigned to the appropriate hosts when powered on.

- **Place VMs in Capacity Reservation Groups**: Select this option to place the VMs in a capacity reservation group.

> **Note:** See Manage Capacity Reservations Groups for full details.

  - **Capacity Reservation Groups**: From the drop-down list, select the capacity reservation group(s).

- **Deallocate powered off but not deallocated VMs**: Select this option to have a periodic task check if any session host VMs are in a powered off (but not deallocated) state and automatically deallocate them to save on Azure compute costs.
- **Install App Attach certificates**: Select this option to install all stored certificates if the App Attach packages are added to this host pool.
- **Install Applications**: Select this option to install applications configured by recurrent UAM policies before moving the host out of drain mode.
- **Restart VM after deployment**: Select this option to restart the VM after it is created.

> **Note:** If certain extensions are installed during deployment (FSLogix, Sepago, Virtual Desktop Optimizations, or User Sessions Time Limits), the VM is automatically rebooted even if this option is not selected.

- **Always prompt for password**: Select this option to always prompt the user for a password.

Note: This policy setting specifies whether Remote Desktop Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users signing in to Remote Desktop Services, even if they already provided the password in the Remote Desktop Connection client.

By default, Remote Desktop Services allows users to automatically sign in by entering a password in the Remote Desktop Connection client.

- If you select this option, users cannot automatically sign in to Remote Desktop Services by supplying their passwords in the Remote Desktop Connection client. They are prompted for a password to sign in.
- If you do not select this option, users can always sign in to Remote Desktop Services automatically by supplying their passwords in the Remote Desktop Connection client.

- **Enable encryption at host**: Select this option so that data stored on the session host VMs is encrypted at rest and flows encrypted to the Storage service.

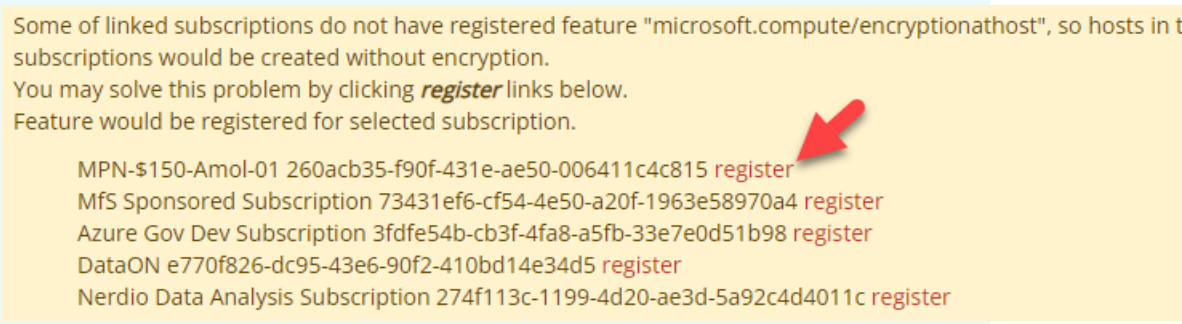
Notes:

- This setting only applies to newly created desktops.
- Encryption sets are per subscription/region. You can create hosts in different subscriptions/regions, and based on the host's subscription/region we select the appropriate encryption set.
- See this Microsoft article to learn more about the encryption at host feature.

- **Register**: If necessary, select this option to register the feature "microsoft.compute/encryptionathost" with the linked subscriptions that do not have this feature.

Notes:

- Nerdio Manager supports the use of both platform-managed keys (default) and customer-managed keys (Encryption Sets). If you are using Encryption Sets, these must be created in the same region as the target session host VMs.
- If this subscription was registered in Nerdio Manager using the "logged in user" option, you must use an account with Subscription Owner permissions to register these features.
- If this feature is not registered, hosts in the linked subscriptions would not have encrypted data.
- This is a sample pop-up warning message:



- **Enable boot diagnostics**: Select this option to apply the Boot Diagnostics feature to desktops in this pool.

Note: This setting only applies to newly created desktops.

- **Storage accounts for boot data**: Optionality, from the drop-down list, select an available storage account to be used to store boot data.

Note: By default, Azure uses an automatic managed storage account for screen shots and other data. To use the default setting, leave this empty.

- **Enable watermarking**: Select this option to enable watermarking.

> **Note:** Watermarking helps prevent sensitive information from being captured on client endpoints. When you enable watermarking, QR code watermarks appear as part of the remote desktops. The QR code contains the connection ID of a remote session that admins can use to trace the session.

  - **Scale**: Select the scale, which is the size in pixels of each QR code dot. This value determines the number of squares per dot in the QR code.
  - **Opacity**: Select the opacity, which is how transparent the watermark is, in percent, where 0 is fully transparent.
  - **Width factor**: Select the width factor which determines the distance between the QR codes in percent. When combined with the height factor, a value of 0 would make the QR codes appear side-by-side and fill the entire screen.
  - **Height factor**: Select the scale, which determines the distance between the QR codes in percent. When combined with the width factor, a value of 0 would make the QR codes appear side-by-side and fill the entire screen.
- **Enable Hibernation**: Select this option to save time and money by deallocating your virtual machine and saving the contents of its RAM to the root volume, allowing you to resume from where you left off when your VM restarts.
- **Security Type**: From the drop-down list, select the security type.

> **Note:** Security type refers to the different security features available for a virtual machine. Security features like Trusted Launch and Confidential virtual machines improve the security of Gen2 VMs. However, additional security features have some limitations, which include not supporting back up, managed disks, and ephemeral OS disks.

- **Secure Boot**: Select this option to enable Secure Boot, which helps protect your VMs against boot kits, rootkits, and kernel-level malware.

- **vTPM**: Select this option to enable Virtual Trusted Platform Module (vTPM), which is TPM 2.0 compliant and validates your VM boot integrity apart from securely storing keys and secrets.
- **Integrity Monitoring**: Select this option to enable cryptographic attestation and verification of VM boot integrity along with monitoring alerts if the VM didn't boot because the attestation failed with the defined baseline.
- **Entra ID group(s)**: From the drop-down list, select the default Entra ID group(s) to add the session hosts to.
- **Enforce Intune Compliance** : Select this option to make hosts unavailable to users until the Intune compliance requirements are met.

> **Note:** You may select that all Intune policies are met or only compliance policies are met. In addition, enabling this feature may result in significant increase in provisioning time, depending on the configured Intune compliance requirements.

- **Allow non-admin users to shadow sessions**: Toggle on this option to enable selected non-admin users or groups to shadow sessions.

> **Note:** Session shadowing is only available with multi-session versions of Windows OS. This feature does not work with Windows 10 Enterprise (single session).

  - **User or Group Name**: From the drop-down list, select the users or groups to allow to shadow sessions.

- **Run scripted actions when...**: Toggle on the desired run script options.

  For each option, enter the following information:

- **Script**: From the drop-down list, select the scripts to execute.

> **Note:** You can select both Windows scripts and Azure Runbooks. In addition, you can drag and drop the scripts to change the order in which they are run.

- **Scripted actions input parameters**: If necessary, provide the required parameters.
- **Pass AD credentials**: Select this option to pass AD credentials.
- **AD Credentials**: From the drop-down list, select the AD credentials to pass.

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

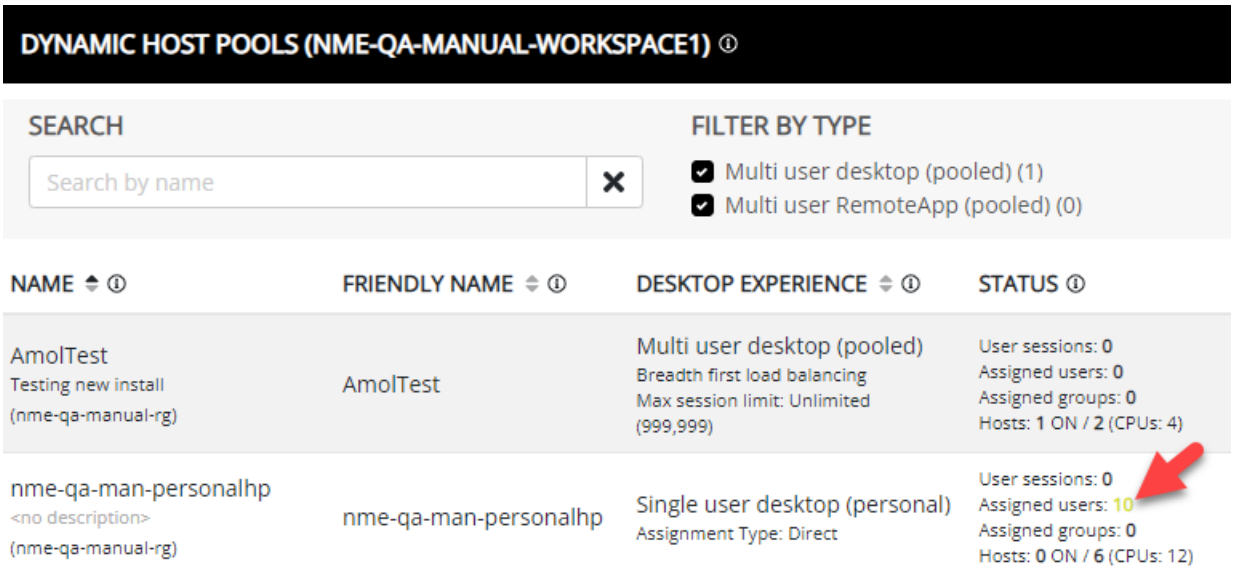
Manage Host Pool User Assignments

> **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.

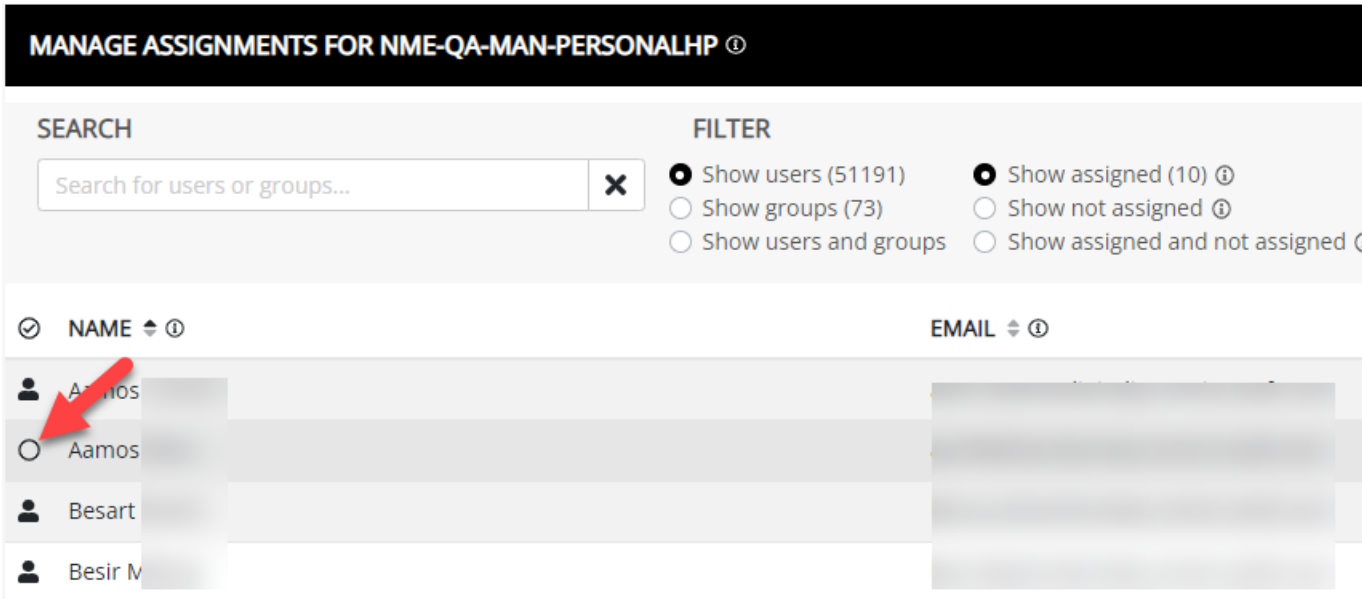
Nerdio Manager allows you to view users assigned to various host pools. In addition, you can assign or unassign users from the host pool.

To manage host pool user assignments:

1. Locate the host pool you wish to work with.
2. In the **Status** column, select the number next to **Assigned Users** to view the users and groups.



3. In the **Manage Assignments** window, you may search, sort, and filter the users and groups. For example, filter for all users not assigned to the host pool.
4. To unassign users from the host pool, select the icon next to the user(s) you wish to unassign.



5. When you have selected all the users, select **`Unassign`**.

6. To assign users to the host pool, select the icon next to the user(s) you wish to assign.
7. When you have selected all the users, select **`Assign`**.

Configure the Host Pool's Active Directory Settings

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.

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`**.

Start VM on Connect for Pooled 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.

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

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 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

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.

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

Add App Groups to Host Pools

Application Groups allow the assignment of users and groups to desktops and RemoteApps. This helps simplify application management because applications can be managed by app groups instead of individual users.

Note: There must be at least one app group associated with a host pool.

To add an app group to a host pool:

1. Select the host pool you want to work with.
2. From the action menu, select **Manage** > **App groups**.
3. Enter the following information:

- **RemoteApp app groups**: Type the name(s) of the app groups for RemoteApps.

> **Note:** A host pool may have multiple RemoteApp app groups.

- **Desktop app group**: Type the name of the Desktop app group.

> **Note:** A host pool may only have one Desktop app group.

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

Publish RemoteApps to Users

RemoteApps gives the user the ability to launch a single application without having to launch the full desktop experience. For example, the user can launch Excel without having to sign in to a desktop. This saves on session host resources because the users do not have to use a full desktop. So, in our Excel example, you might be able to have 10 users working with Excel as a RemoteApp, but had the users connected as a full desktop, the session host might have been able to handle fewer users. That means you would have to deploy additional session hosts to handle all the Excel users.

To publish a remote application to users:

1. Select the host pool with RemoteApp (Pooled) you want to work with.
2. From the action menu, select **Applications** > **RemoteApps**.
3. Select **Add RemoteApp**.

Notes:

- When adding the RemoteApp, the host must be switched on and the applications that you want to publish must be already installed.
- If the host pool has multiple RemoteApp app groups, a specific RemoteApp app group must be selected. By publishing different applications to different Application Groups, administrators can control access to these applications via group membership. This allows user groups to be served different applications from the same host pool.

4. Enter the following information:
   - **Application Source**: From the drop-down list, select application's source.
   - **Application**: From the drop-down list, select the application.
   - **Name**: Type the name of the RemoteApp.

     Note: The **Name** is visible to the user unless overridden by the **Friendly Name**.

   - **Friendly Name**: Optionally, type the friendly name that is visible to the user.
   - **Description**: Type the description that is visible to the admin.
   - **File Path**: Type the path to the application executable on the session host.
   - **Icon Path**: Optionally, type the path to an icon file to be used for this RemoteApp when it appears in the user's Remote Desktop feed.
   - **Icon Index**: Optionally, type the numeric icon index in the icon file.

     For Installed on Host:

     - **Command Line Setting**: Select this option to require a command line setting.

       Note: This option should be selected if a command line value is required.

- **Command Line**: Type the command line to pass to the executable when launching the RemoteApp.

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

   The authorized host pool users now need to be assigned to the RemoteApp Group that contains the newly published RemoteApp.

> **Note:**
>
> - Host pool users are not automatically assigned to that host pool's RemoteApp Groups. Each user must be individually assigned to the appropriate RemoteApp Group.
> - From the action menu, you can **Edit** or **Delete** published apps.

Related Topics

Remote Applications Maintenance Mode

Step #4: Storage

The next step is to configure Storage.

This section discusses topics related to Azure Files and Azure NetApp Files management.

Azure Files and Azure NetApp Files are a native Azure service often used instead of a traditional IaaS-based virtual machine acting as a file server. It is a more flexible approach offering configurable throughput, including input/output performance characteristics. Azure Files is often used in combination with a user profile management solution such as FSLogix.

Nerdio Manager enables you to work with existing Azure File shares, by linking these to Nerdio Manager. Alternatively, Nerdio Manager can create a completely new Azure Files file share for you, including things such as adding permissions, joining it to the domain, and more.

Nerdio Manager also offers some unique management features not found anywhere else. A great example of this is the ability to auto-scale your Azure Files file share, meaning you are only charged for the storage you consume and you do not have to over provision your file shares leading to higher monthly costs.

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*.

Additional Notes:

- 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.

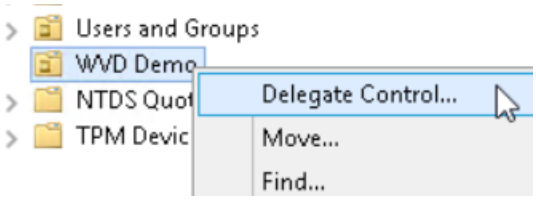
Azure Files joins the domain as a delegated service principal user object. In order to join the Azure Files storage account to the domain, the provided service account requires permissions on the target Organizational Unit (OU) that allows creating and writing new user objects. In addition, the service 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

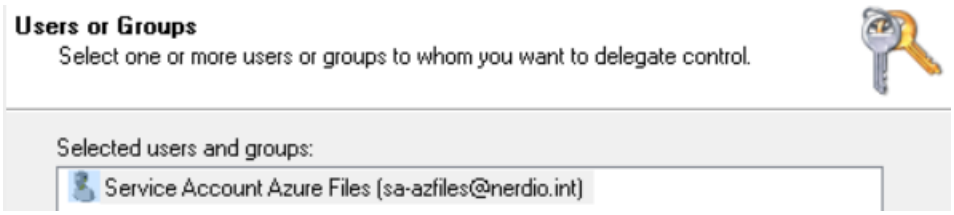
The following procedure describes how to delegate permission to create and write user objects using Active Directory Users & Computers (ADUC, or dsa.msc).

To delegate permission to create user objects:

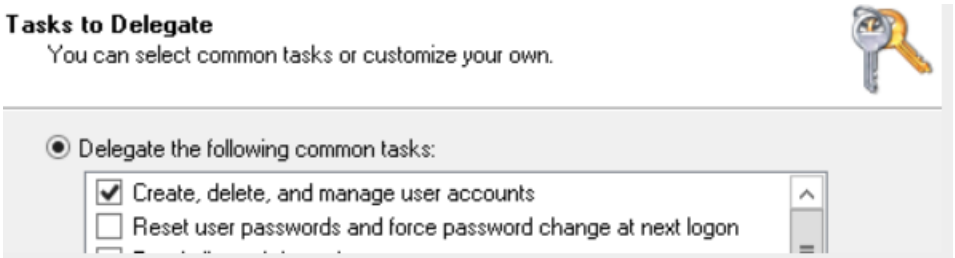
1. Locate the OU where Azure Files are to be joined.
2. Right-click the OU and select **Delegate Control**.



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.

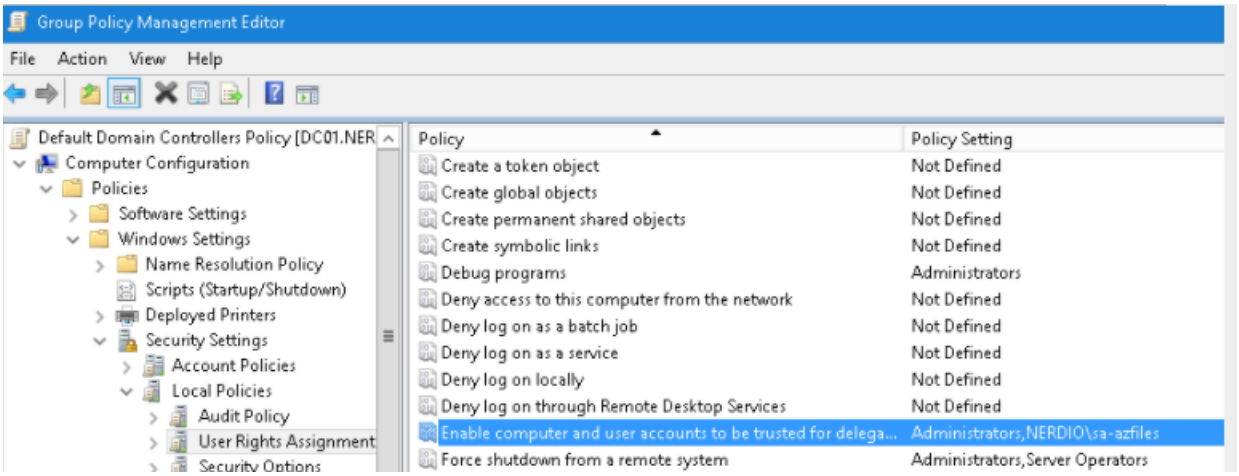
Delegate Permission to Create Delegated Users

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.

To link to an existing Azure Files file share:

1. Navigate to **Storage** > **Azure Files**.
2. Select **`Link Azure Files`**.
3. Enter the following information:
    - **Storage Account**: From the drop-down list, select the storage account.
    - **File Share**: From the drop-down list, select the file share.
4. Once you have entered all the desired information, select **`OK`**.

    After a few moments, the Azure Files file share is added to Nerdio Manager.

To create a new Azure Files file share and/or storage account:

1. Navigate to **Storage** > **Azure Files**.
2. Select **`Add Azure Files`**.
3. Enter the following information:
    - **Storage Account**: From the drop-down list, select the storage account.
    - **Storage Account Description**: Type the description of the storage account.
    - **Resource Group**: From the drop-down list, select resource group for the storage account and Azure Files share.
    - **Performance**: From the drop-down list, select performance tier for the share.

> **Tip:** It is strongly recommended that you select **Premium** for the best user experience.

- **Replication**: From the drop-down list, select the type of storage replication.

> **Note:** See this Microsoft article for more information about Azure storage redundancy.

- **File Share Name**: Type the share's name.
- **File Share Description**: Type the share's description.
- **Provisioned Capacity (GiB)**: Type the size of the provisioned capacity.
- **Share-level permissions**: Select this option to set default share-level permissions on storage account.

> **Note:**
>
> - **SMB Share Contributor** permission can be used to allow all authenticated users read/write access to the share.
> - **SMB Share Reader** can be used to allow all authenticated users read-only access to the share (for example, MSIX app attach).
>
> See this Microsoft article for additional information.

- **Permissions (SMB Share Contributors)**: Specify users/groups that have Storage File Data SMB Share Contributor role on the share.

> **Note:** This is required for read/write access to the share.

- **Add users / groups from host pools**: From the drop-down list, select users/groups currently assigned to these host pools to be given Storage File Data SMB Share

Contributor role on the share.

- **Join to AD or Entra ID**: Select this option and then from the drop-down list, select an Entra ID or an AD profile to directly join the share.

> **Note:** To use an Azure Files share as a storage location for FSLogix profiles and MSIX App Attach images, the storage account must be integrated with Active Directory, Entra Domain Services, or Entra ID. If you select not to join the storage account to AD or Entra ID, you can do so later. Joining the storage account to AD creates a temporary VM and uses the AD profile credentials to add the storage account as a Computer object in selected AD. Integrating storage account with Entra Domain Services sets the appropriate flag in Azure. Entra Domain Services admin profile credentials are necessary to create a temporary VM to be domain-joined and enable AES-256 encryption. Joining the storage account with Entra ID creates the necessary app registration and provides you with an option to grant needed consents.

- **Create a computer-joined file share**: Select this option to join Azure Files storage accounts to AD by creating either a user object or a computer object in Active Directory.

> **Note:** It is recommended that a user object is used for the domain join process. Please ensure that no policies are in effect that may disable or remove this account or reset its password. If a computer object is selected, ensure this account is excluded from any automated cleanup process. All file shares are created with AES256 encryption enabled.

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

Notes:

- This is in addition to assigning Azure RBAC roles selected above.
- This process automatically creates a temporary VM to perform the permission assignment task.
- See this Microsoft article for information about default file permissions used on new Azure Files shares.

  - **App Attach**: Select this option to grant Authenticated Users Read permission to sub-directories in the share. This is recommended for shares containing App Attach applications.
  - **FSLogix**: Select this option to grant Authenticated Users Modify permission to the root directory in the share, allowing for the creation of FSLogix profile folders. This is recommended for shares containing FSLogix profiles.

- **`Show advanced settings`**: To join Azure Files to the Active Directory Nerdio Manager creates a temporary VM to perform the operation. Select the settings to be used for this temporary VM.

Tip: It is strongly recommended that you allow Nerdio Manager to use the default settings when creating the temporary VM. That is, we recommend that you do not use the advanced settings.

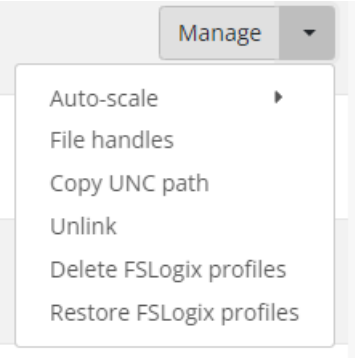
- **Enable SMB Multichannel**: Select this option to improve the Azure Files Premium performance.
- **Apply tags**: Optionally, type the **Name** and **Value** of the Azure tag to apply to the Azure Files share.

Note: You may specify multiple tags. See this Microsoft article for details about using tags to organize your Azure resources.

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

To manage configured Azure Files shares:

1. Navigate to **Storage** > **Azure Files**.
2. Locate the Azure Files share you want to manage.
3. The action menu allows you to perform the following functions:



   - **Manage**: Manage the file share's configuration.
   - **Auto-scale**: See "Auto-scale for Azure Files Storage Premium" on the next page for more information.
   - **File handles**: Unlock files/Close open file handles.
   - **Copy UNC Path**: Copy the UNC path to the clipboard.
   - **Unlink**: Remove the Azure Files file share from Nerdio Manager.
   - **Delete FSLogix Profiles**: Delete a selected FSLogix profile.
   - **Restore FSLogix Profiles**: Restore a selected FSLogix profile that was previously deleted.
4. From the action menu, select **Manage** to change the Azure Files share's parameters and permissions.

Related Topics

"Create and Manage Configured Azure NetApp Files" on page 159

Auto-scale for Azure Files Storage Premium

A premium file share is billed by provisioned size, regardless of the capacity used. Share sizes can range from 100 GiB to 102,400 GiB. IO and network bandwidth limits scale with the provisioned share size.

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

Storage auto- scaling with Azure Files can also be used to maintain a specified headroom to avoid running out of space on the volume or capacity pool.

Note: Auto-scale is not available for Azure Files standard storage, because both capacity cost and performance are not controlled by the size of the share.

You must configure these auto-scale parameters:

- Provisioned Size (Quota)
- Scheduled Data Increase (Optional)
- Scaling Logic

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

1. Navigate to **Storage** > **Azure Files**.
2. Locate the files share you want to manage.
3. From the action menu, select **Auto-scale** > **Configure**.
4. Toggle the **Auto-Scale** option to **On**.
5. Enter the **Provisioned Size (Quota)** settings.
    - **Quota unit**: From the drop-down list, select the unit (Relative % or Absolute GiB). Relative is a percentage of currently used capacity.
    - **Minimum size**: Type the minimum size in GiBs or %.

> **Note:** The minimum size is 100 GiB and it may not be smaller than the used capacity. In addition, this defines the minimum buffer that the system always maintains as the user capacity grows. This guarantees the minimum amount of free space in the file share.

- **Maximum size**: Type the maximum size in GiBs or %.
    - **Less than**: Type the size the file share should be increased, below the total file share size, to prevent the uncontrolled system growth..

The **Performance** displays the minimum and maximum configuration values, and displays the performance characteristics.

6. Optionally, toggle **Scheduled Quota Increase On** and enter the settings.

> **Note:** These are the parameters by which you are committed to increase the scheduled quota. The quota is increased during this period and decreased between these periods. This is useful if you have days with peak performance.

- **Days**: From the drop-down list, select the range of days.
- **Hours**: From the drop-down list, select the time zone.
- **Set provisioned size (quota) to**: Type the quota that you commit to increase above the current used capacity.

7. Enter the **Scaling Logic** settings.

> **Note:** Provisioned size (quota) can be decreased only 24 hours after the last quota increase. The quota is increased at the beginning of the period and decreased to the minimum size only at the end of this period.

- **Select auto-scale trigger**: From the drop-down list, select the trigger.

  > **Note:** The auto-scale logic configuration allows the scaling engine to determine when to grow or shrink the share. It is based on two available metrics provided by Azure files shares via the API. It describes how long it takes the IOPs to be processed. It can either be the Average Success Server Latency (default) or the Maximum Success Server Latency.

- **Increase the quota (scale out) by**: Type the size the quota is increased according to the Quota unit value specified in the **Provisioned Size (Quota)** section.

  > **Note:** When threshold is exceeded, the system continues scaling out until either it reaches the specified Max size, or until the server latency is below the threshold.

- **Decrease the quota (scale in)**: Type the size the quota is decreased if the server latency drops below the specified threshold.

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

   The configured file share appears in the list of shares on the **Azure Files** list.

Related Topics

"Auto-scale for Azure NetApp Files" on page 161

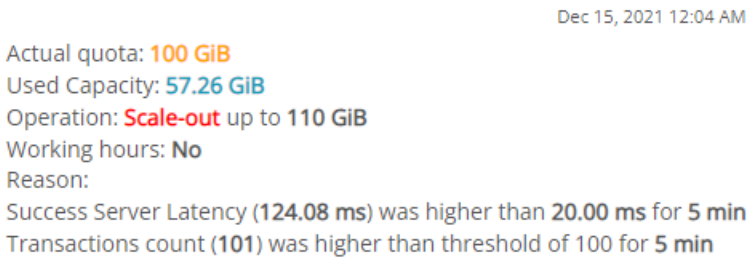
Auto-scale History for Azure Files Shares

The auto-scale history visualization helps you understand auto-scale behavior and how it impacts your deployment.

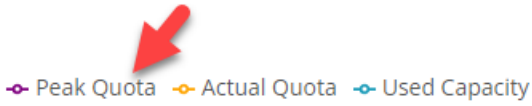
The following are important auto-scale history features.

- **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:



- **Action Points**:
  - **Scale Out**: This action point indicates that a scale-out event took place. (Red indicates that the scale-out event is costing money.)
  - **Scale In**: This action point indicates that a scale-in event took place. (Green means that the scale-in event is saving money.)
  - **Azure Issue**: This indicates that there was a problem communicating with Azure. If this occurs frequently, please contact Nerdio Manager technical support.
- At the bottom of any graph, select the data set name to toggle on/off the display line associated with that information. For example, select **Peak Quota** to suppress that line on the graph. Select it again to display it.



To view auto-scale history for an Azure Files share:

1. Navigate to **Storage** > **Azure Files**.
2. Locate the file share you wish to work with.

3. From the action menu, select **Auto-scale** > **History**.
4. Select the desired time range and the specific graphs to display.
    - **Quota (GiB)**: The Quota graph displays the following information about the file share quota:
        - **Peak Quota**: The maximum size of the quota.
        - **Actual Quota**: The actual quota size as it is currently configured.
        - **Used Capacity**: The actual storage used.
    - **Latency (ms)**: The Latency graph displays the following information:
        - **Server Latency (avg)**: The average time used to process a successful request by Azure Storage. This value does not include the network latency specified in the End-to-End Latency.
        - **End-to-End Latency (avg)**: The average end-to-end latency of successful requests made to a storage service or the specified API operation. This value includes the required processing time within Azure Storage to read the request, send the response, and receive acknowledgment of the response.
    - **Transactions**: The Transactions graph displays the number of transactions.
    - **Savings%**: The Savings graph displays the savings percentage.

Related Topics

"Auto-scale History for Azure NetApp Shares" on page 165

Create and Manage Configured Azure NetApp Files

This feature is only available in the Nerdio Manager **Premium** edition.

The **Azure NetApp Files** page contains a list of all the configured and linked Azure NetApp files shares. You can perform various actions on the files shares such as creating or managing files shares.

To link to an existing Azure NetApp Files share:

1. Navigate to **Storage** > **Azure NetApp Files**.
2. Select **`Link ANF Volume`**.
3. From the drop-down list, select the **NetApp Files Account**.
4. Select **`OK`**.

   After a few moments, the Azure NetApp Files file share is added to Nerdio Manager.

Create an Azure files and/or storage account.

Note: Before proceeding, verify that ANF is available in your Azure region and that your Azure subscription is whitelisted for this service.

1. Navigate to **Storage** > **Azure NetApp Files**.
2. Select **`Add ANF Volume`**.
3. Enter the following information:
   - **Active directory**: From the drop-down list, select the active directory.
   - **Resource group**: From the drop-down list, select the resource group.
   - **Network**: From the drop-down list, select the network.
   - **Subnet**: From the drop-down list, select the subnet.
   - **AD-aware DNS Server**: Type the address of the AD-aware DNS server.
4. Once you have entered all the desired information, select **`Next`**.
5. Enter the following information:
   - **Resource group for ANF account**: From the drop-down list, select a resource group to contain the Azure NetApp Files account objects.
   - **Account name**: Type the ANF account name or leave it blank for it to be automatically generated.

- **SMB server prefix**: Type the prefix of the computer objects that are to be joined to the AD domain and used for the UNC path. For example: **SMB- PREFIX** - random\volume\share\folder.
- **Volume name**: Type the volume name to be created on the SMB server specified above.

> **Note:** There can be multiple volumes in the same ANF account.

- **Capacity (TiB)**: Type the capacity in TiB.

> **Note:** The minimum capacity of an ANF capacity pool is 4 TiB.

- **Performance Tier**: From the drop-down list, select the performance tier of the new capacity pool and volume.

> **Note:** Performance tiers vary in price and throughput (IOPS). See the following Microsoft document for details.

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

Related Topics

"Create and Manage Configured Azure Files Shares" on page 150

Auto-scale for Azure NetApp Files

> This feature is only available in the Nerdio Manager **Premium** edition.

In Azure storage NetApp files, you have an ANF account that can have multiple capacity pools. Capacity pools are created with a service level (Standard, Premium, Ultra) that determines performance. Within each capacity pool you can have one or more volumes that, in aggregate, cannot exceed the size of this capacity pool. The cost of the ANF storage is determined by the

size of the capacity pool, with the minimum size of 4 TiB. You can grow and shrink a capacity pool in increments of 1 TiB, but not smaller than the sum of the volumes that are contained within that capacity pool.

The throughput limit of the ANF storage system is determined by a combination of the quota assigned to the volume and the service level selected.

Storage auto-scaling with ANF is required when you need to dial-up the performance of a particular volume during times of high demand on the storage system, and then dial it back down, on a scheduled basis, when that performance is no longer needed. For example, during sign in/sign out storms from Azure VD machines. Or it could be needed when there is heavy activity on the storage system in the middle of the day and the latency of that volume is detected to be high.

Storage auto- scaling with ANF can also be used to maintain a specified headroom to avoid running out of space on the volume or capacity pool.

To configure and manage auto-scale for Azure NetApp files:

1. Navigate to **Storage** > **Azure NetApp Files**.
2. Locate the ANF you want to manage.
3. From the action menu, select **Auto-scale** > **Configure**.
4. Toggle the **Auto-Scale** option to **On**.
5. Enter the **Provisioned Size** settings.

> **Note:** If the volume free space drops below the Min, the system tries to grow the volume. If it cannot grow the volume within the current capacity pool, the capacity pool is always expanded by 1 TiB, and the volume grows at least for 1 TiB.
>
> The volume won't grow beyond the configured maximum size.

- **Mode**: From the drop-down list, select the mode:
  - **Volume only**: Auto-scales the volume without the capacity pool that contains it. The volume is limited to the available free space within the capacity pool,

and the capacity pool does not increase automatically.

- **Volume and capacity pool**: Auto-scales the volume and the capacity pool that contains it (default).

- For **Volume only**:
  - **Size unit**: From the drop-down list, select the unit (Relative % or Absolute GiB). Relative is a percentage of currently used capacity.
  - **Minimum size**: When scaling down, type the minimum size to maintain on the volume. This is evaluated as the currently used capacity + headroom amount.

    Note: If the available space drops below the configured minimum free space, the volume is increased to meet the minimum available space. If exceeding capacity pool size, and capacity pool scaling is enabled, then an additional 1 TiB is added to the capacity pool to increase the volume – up to the configured maximum total size.

  - **Maximum size**: When scaling out, type the maximum amount the volume should increase. This is evaluated as the currently used capacity + the scaling amount.
    - **Less than**: Define the Max size the volume may grow in order to prevent the uncontrolled system growth. This is limited by the available capacity pool size.

- For **Volume and capacity pool**:
  - **Minimum volume free space**: Type the minimum free to maintain on the volume. If the current free space falls below this threshold, the volume automatically grows along with the capacity pool.
  - **Maximum volume total size**: Type the maximum volume size of the volume in TiBs. The volume and capacity pool combination cannot grow larger than this value.

- **Exceeding the limit should trigger an error**: Select this option to have the auto-scale process trigger an error if the calculated size exceeds the maximum limit.

> **Note:** This allows you to track these errors using notifications. See Configure Email Notifications for details.

The **Size and Performance** calculator displays the minimum and maximum configuration values and displays the performance characteristics.

6. Optionally, toggle **Scheduled-Based Scaling On** and configure the settings.

> **Note:** This is useful if you have peaks in demand on the storage system (for example, when multiple users sign in and sign out during the same time). You can specify more than one period of the peak auto-scaling, after which the system automatically scales down to the Min size. Be sure that the schedules do not overlap.

- **Time Zone**: From the drop-down list, select the time zone.
- **Days**: From the drop-down list, select the days.
- **Hours**: From the drop-down list, select the range of hours.
- **Set provisioned size to**: Type the amount of additional capacity to add to the volume, beyond the current capacity.

7. Optionally, toggle **Latency-Based Scaling On** and configure the settings.
   - **Select auto-scale trigger**: From the drop-down list, select the trigger.

> **Note:** This is the average or maximum time used to process a successful request by Azure Storage.

   - **Increase volume size (scale out)**: The system increases the volume size by the value that you set if the server latency exceeds the specified threshold.

- **Decrease volume size (scale in)**: The system decreases the volume size by the value that you set if the server latency drops below the specified threshold.

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

   The configured file appears in the list of files on the **Azure NetApp Files** list.

Related Topics

"Auto-scale for Azure Files Storage Premium" on page 155

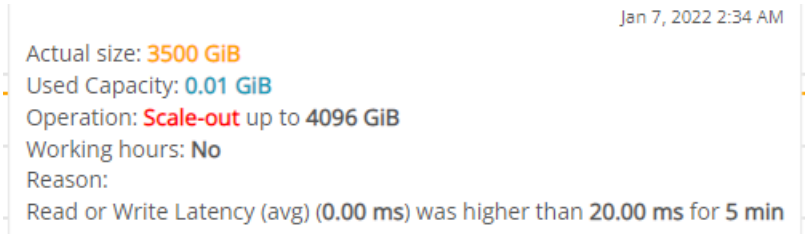
Auto-scale History for Azure NetApp Shares

This feature is only available in the Nerdio Manager **Premium** edition.

The auto-scale history visualization helps you understand auto-scale behavior and how it impacts your deployment.

The following are important auto-scale history features.

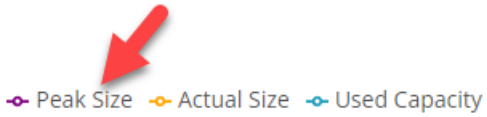
- **Time Range**: At the top of the window, select the desired time range to display.
- **Show**: At the top of the window, select the desired graph(s) to display.
- **Savings**: At the top of the window, you can view auto-scale savings.
- **Zoom In**: For the **Size (GiB)** graph only, click and drag the mouse over the section of the graph you wish to zoom in on. When you are zoomed in, select **`Zoom-out`** to restore the full graph.
- **Hover**: You can hover over any part of any graph to see its details. For example:



- **Action Points**:

- **Scale Out**: This action point indicates that a scale-out event took place. (Red indicates that the scale-out event is costing money.)
- **Scale In**: This action point indicates that a scale-in event took place. (Green means that the scale-in event is saving money.)
- **Azure Issue**: This indicates that there was a problem communicating with Azure. If this occurs frequently, please contact Nerdio Manager technical support.

- At the bottom of any graph, select the data set name to toggle on/off the display line associated with that information. For example, select **Peak Size** to suppress that line on the graph. Select it again to display it.



To view auto-scale history for an Azure NetApp share:

1. Navigate to **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" on page 157

Step #5: FSLogix and User Profile Management

The next step is to configure FSLogix and User Profiles.

FSLogix and User Profile Management

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

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

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

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

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

Nerdio Manager makes sure that setting up, configuring, and managing FSLogix Profile Containers is easy to do. Multiple so-called FSLogix configuration profiles can be created, which can be applied per host pool. This means you can have different FSLogix configurations where, for example, the storage locations are different (often in the form of Azure Files, see "Create and Manage Configured Azure Files Shares" on page 150 for more information) or where you have different registry parameters set, again, on a per-host pool level.

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

Related Topics

"FSLogix Settings and Configuration" below

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.

To add an FSLogix Profiles Storage configuration:

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

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

> **Note:** See the following Microsoft article for more information about FSLogix Cloud Cache.
>
> Cloud Cache allows you to specify multiple profile storage location. It asynchronously replicates the profiles and makes the profiles available in multiple storage locations at the same time. So, if one of the locations is not available, the session host automatically fails over to one of the alternate locations.

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

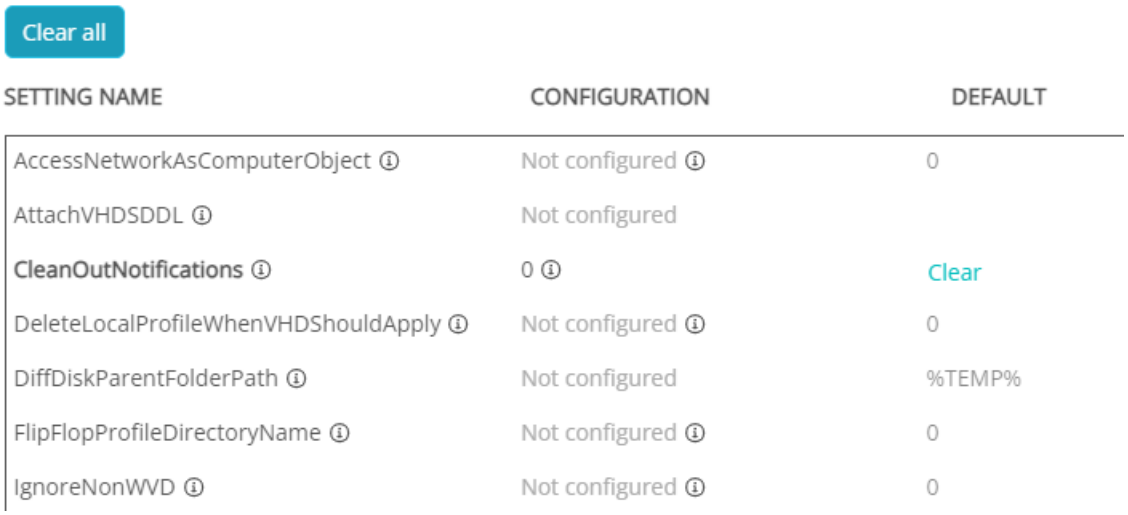
> **Note:** See this Microsoft article for more information.

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

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

- **FSLogix Registry Options**: From the drop-down list, select whether you want to work with **All settings** or **Advanced**.

- For **All settings**:



  - In the **Configuration** column, type the setting's value.
  - Select **`Clear`** to set a specific setting to **Not configured**.
  - Select **`Clear all`** to set all the settings to **Not configured**.
- For **Advanced**:
  - You can add DWORD values in the format: *"ValueName":dword:ValueData (example: "ProfileType"=dword:00000003)*.
  - You can add string values in the format: *"ValueName":"ValueData" (example: "VolumeType":"vhdx")*.

- **Configure Office Container to redirect Microsoft 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**: Modify as needed.

- **Redirections**: Select this option if you want to include Redirections in the global profile for re-use across customers.

> **Note:** See this Microsoft article for more information about redirections.

- **Force the installation of FSLogix apps even if already installed**: Select this option to force the re-installation of the FSLogix agent and applications.

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

To set Nerdio Manager to install the FSLogix application automatically:

1. Navigate to **Settings** > **Integrations**.
2. In the **FSLogix Profiles storage** tile, add, change, and remove the profiles as needed.

> **Notes:** Be sure to select the following options for FSLogix profiles linked to hybrid host pools.
>
> - **Use Cloud Cache**: Select this option to enable FSLogix Cloud Cache in the host pools, and the session hosts within those host pools, that use this FSLogix profile.
> - **Use Azure page blobs**: Select this option to use storage account blob containers to store users profiles. These containers are accessed using storage account access keys.

3. Select one profile as the default.

Notes:

- If you set the **Use FSLogix Profiles** option to **Off**, the FSLogix app is installed automatically when new hosts are created or re-imaged.
- Each host pool's FSLogix settings can be customized.
- FSLogix is not installed on the desktop image.
- The FSLogix registry settings are not set on the desktop image.
- No environment has GPO to control the FSLogix configuration.

To manage FSLogix installation and configuration manually:

1. Locate the host pool you wish to change.
2. From the action menu, select **Properties** > **FSLogix**.
3. Toggle **Use FSLogix profiles** to **Off**.
4. Select **`Save & close`**.
5. The application must be installed on the desktop image.
6. The configuration must be applied either via the registry on the desktop image or with a GPO.

To change the FSLogix registry options:

1. Locate the host pool you wish to change.
2. From the action menu, select **Properties** > **FSLogix**.
3. Make the changes to the FSLogix registry options.

Notes:

- 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")*.

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

Note: These values are added under the **HKLM\SOFTWARE\FSLogix\Profiles** key. See the above link for Microsoft documentation on the FSLogix profile container registry reference.

Related Topics

"FSLogix and User Profile Management" on page 168

Automated FSLogix Deployment and Per-Host Pool Customization

You can configure FSLogix with Nerdio Manager and apply its settings to each host pool in the WVD Deployment.

For more information refer to "Host Pools" on page 76.

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 global settings for FSLogix:

Note: FSLogix settings configured here are automatically installed and fully deployed to any newly created host pools.

1. Navigate to **Settings** > **Integrations**.
2. In the **FSLogix Profiles storage** tile, locate the profile you want to use as the default.
3. Select **`set default`**, if it isn't already the default.
4. Select the profile and enter the following information:
    - **Name**: Type the profile's name.
    - **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 a testing scenarios.)

      Note: See the following Microsoft document for more information about FSLogix Cloud Cache.

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

    - **Use Azure page blobs**: Select this option to use storage account blob containers to store users profiles. These containers are accessed using storage account access keys.
    - **Configure session hosts registry for Entra ID joined storage**: Select this option to enable Entra ID Kerberos functionality and Entra ID account credentials loading.

      Note: See this Microsoft document for more information.

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

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

- **FSLogix Registry Options**: Type the FSLogix configuration that is applied when a session host VM is provisioned and FSLogix is installed.
    - **Edit mode**: From the drop-down list, select the edit mode.

> **Note:** Select **all settings** to edit in "simple" mode, removing the need to configure registry settings individually. Select **Advanced** to configure the registry settings as usual.

- **Force the installation of FSLogix apps even if already installed**: Select this option to force the reinstallation of the FSLogix agent and applications.

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

To configure customized FSLogix settings for a host pool:

> **Note:** Any settings configured here are applied only to newly created or re-imaged hosts in this pool.

1. Navigate to the list of host pools and locate the host pool you wish to change.
2. From the action menu, select **Properties** > **FSLogix**.
3. Enter the following information:
    - Toggle **Use FSLogix profiles** to **On**.

> **Note:** If this option is not enabled, Nerdio Manager does not install the FSLogix profile container application on newly created VMs when they are deployed in this host pool. Existing VMs are not affected.

- **FSLogix profile**: From the drop-down list, select the FSLogix profile to use.
- **Use Cloud Cache**: Select this option to enable FSLogix Cloud Cache.
- **FSLogix Profile path**: Modify as needed.
- **FSLogix Registry Options**: Modify as needed.
    - **Edit mode**: From the drop-down list, select the edit mode.

      Note: Select **all settings** to edit in "simple" mode, removing the need to configure registry settings individually. Select **Advanced** to configure the registry settings as usual.

- **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**: Modify as needed.
- **Force the installation of FSLogix apps even if already installed**: Select this option to force the reinstallation of the FSLogix agent and applications.
- **Apply to existing hosts**: Select this option to apply these changes to existing hosts. Otherwise, the change only effect new or re-imaged hosts.
    - **Process hosts in groups of**: Type the number of concurrent actions to execute during this bulk operation.
    - **Number of failures before aborting**: Type the number of failures that causes the process to stop.

- **Messaging**: Toggle on the Messaging to send messages to active users.
    - **Delay**: From the drop-down list, select the number of minutes to wait after sending the message before starting the process.
    - **Message**: Type the message you want to send to the users.
- **Schedule**: Toggle on the Schedule to apply the changes at a selected time.
    - **Start Date**: Type the date to start.
    - **Time Zone**: From the drop-down list, select the time zone for the Start time.
    - **Start Time**: From the drop-down lists, select the time to start.
    - **Repeat**: From the drop-down list, select the recurring schedule, if desired.

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

        - **Days After**: If you selected **After Patch Tuesday**, type the number of days after Patch Tuesday to run the scheduled task.

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

Related topics

"Host Pools" on page 76

Host Pool Disaster Recovery: You can enable host pool level active/active DR configuration and Nerdio Manager automatically distributes session hosts across two Azure regions. Users are distributed across VMs in both regions as they sign in and FSLogix profiles are automatically replicated using Cloud Cache. In case of an Azure region failure users continue to access VMs in the available region. See this demo for more information.

Manage Installed Applications on 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.

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.

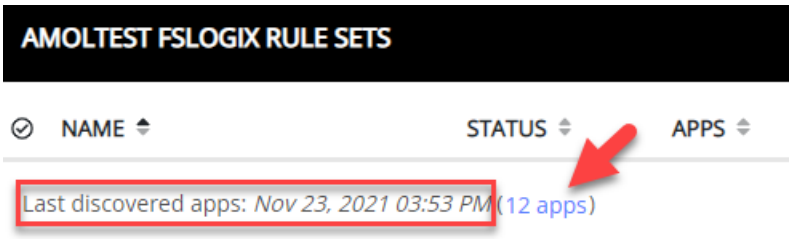
These steps are discussed in detail below.

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:

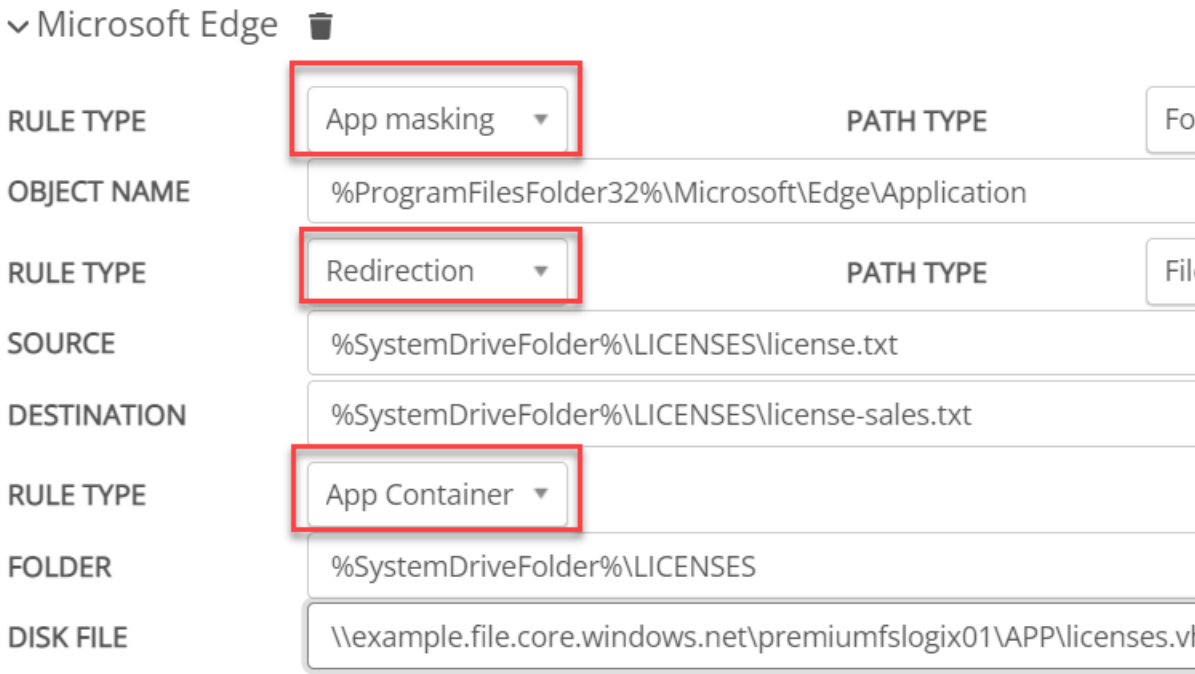
1. Locate the host pool you wish to work with.
2. From the action menu, select **Applications**> **Installed apps**.
3. Select **`Add rule set`**.
4. Enter the following information:

- **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 images.

An MSIX App Attach Image is an expanded container, such as a vhd, vhdx, or cim file, that contains an extracted version of the MSIX packages. An image can contain one or more MSIX packages. The MSIX App Attach images are mounted to the session hosts in the host pool and the applications made available to users who sign in to the session hosts.

Create and Manage MSIX App Attach Images and Host Pool Assignments

This topic discusses how to do the following:

- Upload an MSIX app attach image.
- Upload an MSIX package file.
- Assign an app to a host pool.
- Create a new version of an app.
- Change an app to a new version.

Sample VHD(X) Packages and Certificate

To help you get you started, we created a few VHD(X) packages for some popular applications that you can download and start using in your AVD environment for testing purposes.

Note: These packages are not intended for production purposes. They should be used for proof of concept testing.

Google Chrome

- VHD file MSIX package
- MSIX file

Mozilla Firefox

- VHD file MSIX package
- MSIX file

Notepad++

- VHD file MSIX package
- MSIX file

PuTTY

- VHD file MSIX package
- MSIX file

VLC

- VHD file MSIX package
- MSIX file

Certificate

- The certificate can be downloaded here.
- The certificate is the same for all the packages.

Upload an MSIX App Attach Image File

Nerdio Manager allows you to upload new versions of packages and automatically apply them to existing host pools. In addition, Nerdio Manager can create an image from an existing MSIX package, or you can upload an image file.

To upload an image:

1. Navigate to **Applications** > **App Attach**.
2. Select **`Upload image`**.
3. Enter the following information:
    - **Friendly Name**: Type the name that you want to appear on the images list.
    - **Description**: Type a description.
    - **Storage Location**: From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.

      > **Note:** MSIX App Attach does not support Entra Domain Services or Entra ID. This needs to be Active Directory Domain Services (ADDS).

    - **Version**: Type the version number of the image that you are uploading. This must be unique.
    - **Image File(s)**: Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
    - **Certificate (.cer) File**: Select the certificate file.

      > **Note**: A certificate that was used to create the MSIX package must be installed on all session hosts VMs. If you used a self-signed certificate to create the MSIX package, upload it here and it is automatically installed for you. Alternatively, you can install the certificate on the desktop image and re-image the session host VMs

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

   The image is uploaded to Nerdio Manager.

Upload an MSIX Package File

This feature is only available in the Nerdio Manager **Premium** edition.

If you do not already have a VHD/VHDX./CIM that contains the image, Nerdio Manager allows you to upload the MSIX file and Nerdio Manager automatically creates a VHD file for you.

To upload an MSIX package file:

1. Navigate to **Applications** > **App Attach**.
2. Select **`Upload MSIX app(s)`**.
3. Enter the following information:
    - **Image Name**: Type the image name.
    - **Storage Location**: From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.
    - **MSIX File(s)**: Select the MSIX file(s).
    - **Certificate (.cer) File(s)**: Optionally, select the certificate file(s).

    Note: To expand the MSIX app into a VHDX container, a temporary VM is created to perform the operation and then deleted. It is recommended that you simply let Nerdio Manager handle the temporary VM's configuration. Otherwise, select **`Show advanced settings`** to specify the temporary VM's details.
4. Once you have entered all the desired information, select **`OK`**.

    The MSIX file is uploaded, and Nerdio Manager begins the process of creating a VM to package the file into a VHDX image.

Assign an App to a Host Pool

Once you have uploaded an MSIX app attach image, you can assign the app to a host pool.

To assign an app to a host pool:

1. Locate the host pool you wish to assign the app to.
2. From the action menu, select **Applications**> **MSIX App Attach**.
3. When the **Manage MSIX App Attach** window displays, select **Add**.
4. Enter the following information:
    - **Image Source**: From the drop-down list, select the location of the image that contains MSIX packages. The image can be stored in Nerdio Manager's image library or on any SMB file share that session host VMs have access to. If you have uploaded or created MSIX images using Nerdio Manager, select **Image Library**.
    - **MSIX App Attach Image**: From the drop-down list, select an MSIX App Attach image containing the MSIX packages.
    - **Image Version**: From the drop-down list, select the image's version to be added to the host pool.
    - **Packages**: From the drop-down list, select one or more MSIX packages/apps present in the image to make available to users on this host pool.

    Notes:
    - The package in the file share closest to the host pool's region is prioritized to reduce latency.
    - Ensure that the host pool has at least one running session host VM.
    - Each VM in the host pool must have certificates that were used to sign MSIX installed. Select **`Install certificates`** to install them if they aren't already.
5. Once you have entered all the desired information, select **OK**.

    The MSIX app is added to the host pool.

Assign an App Attach v2 App to Users and Groups

Once you have uploaded an MSIX App Attach v2, you can assign the app to users and groups.

To assign an App Attach v2 app to users and groups:

1. Navigate to **Applications** > **App Attach**.
2. Select the **App Attach v2 packages** tab.
3. Locate the App Attach v2 app you want to work with.
4. From the action menu, select **Users and groups**.
5. From the drop-down list, select the **Users and Groups**.
6. Once you have entered all the desired information, select **OK**.

   The MSIX app is assigned to the users and groups.

Use the App Attach v2 Package Wizard

The App Attach wizard can be used to deploy App Attach packages to all required AVD host pools automatically, without the need to manually deploy packages.

Note: This feature is applicable to App Attach v2 packages only. Ensure that the required Nerdio App Attach image version is replicated to all required regions before proceeding.

To use the App Attach v2 package wizard:

1. Navigate to **Applications** > **App Attach**.
2. Select the **App Attach v2 packages** tab.
3. Locate the App Attach v2 app you want to work with.
4. From the action menu, select **Package wizard**.
5. In the **Image** tab, enter the following information:
   - **Image version**: From the drop-down list, select the image version.
   - **Temporary replica**: From the drop-down list, select the version replica used to extract metadata from the selected App Attach image.

- **Temporary host pool**: From the drop-down list, select the temporary host pool used to expand the image.

> **Note:** A temporary host pool is required as a proxy to extract metadata from the selected App Attach image. No changes are made to the pool configuration and any host pool may be used. However, as best practice we recommend the creation of a dedicated App Attach pool. At least one desktop must be running in the pool to proceed.

6. In the **Package** tab, enter the following information:

   - **Resource group**: From the drop-down list, select the resource group where the App Attach package is created.

> **Note:** This resource group does not need to be in the same region as the pool assignments, but it is recommended as best practice.

   - **Packages**: From the drop-down list, select one or more MSIX packages to make available to users on the selected host pools.

7. In the **Assignments** tab, enter the following information:

   - **Host pools**: From the drop-down list, select one or more host pools from the subscription of the selected resource group that are assigned to the package(s).
   - **Users and groups**: From the drop-down list, select the authorized users and groups to run the applications included in the selected package(s).

8. In the **Summary** tab, review the selections.
9. Once you have reviewed all the desired selections, select **Run**.

   The App Attach wizard task starts. You can see the task's progress in the **App Attach Tasks** window.

Create a New Version of an App

Nerdio Manager allows you to manage multiple versions of an app.

To add a new version of an app:

1. Navigate to **Applications** > **App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.
3. Locate the image you want to add an app to.
4. From the action menu, select **Upload version**.
5. Enter the following information:
    - **Version**: Type the version number of the image that you are uploading. This must be unique.
    - **Image File(s)**: Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
    - **Certificate (.cer) File(s)**: Optionally, select the certificate file(s).

    > **Note**: A certificate that was used to create the MSIX package must be installed on all session hosts VMs. If you used a self-signed certificate to create the MSIX package, upload it here and it is automatically installed for you. Alternatively, you can install the certificate on the desktop image and re-image the session host VMs.

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

    The image is uploaded to Nerdio Manager

Change to a New Version of an App

Nerdio Manager allows you to change to a new version an app.

To change to a new version of an app:

1. Navigate **Applications** > **App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.

3. Locate the image you want to work with.
4. Select **`Image versions`**. The list of image versions displays.
5. Locate the image version you wish to set as the default.
6. Select **`Set as default`**. The confirmation window displays.
7. Select **`Update host pools where this package is assigned`** to assign the new version of the image to the host pools listed above.
8. Select **`OK`**.

   The new version is now the default.

Upload a New Image Version of an App

Nerdio Manager allows you to upload a new image version an app.

To upload a new image version of an app:

1. Navigate **Applications** > **App Attach**.
2. Select either the **Nerdio images** or **App Attach v2 packages** tab.
3. Locate the image you want to work with.
4. From the action menu, select **`Upload a new Image version`**.
5. Enter the following information:
   - **Version**: Type the version number of the image that you are uploading. This must be unique.
   - **Storage Location**: From the drop-down list, select the linked app storage location in the AD-integrated Azure Files share.
   - **Image File(s)**: Select the VHD(X)/CIM file(s) that contains the App Attach application expanded from the MSIX installer.
   - **Certificate (.cer) File(s)**: Optionally, select the certificate file(s).
6. Once you have entered all the desired information, select **`Upload`**.

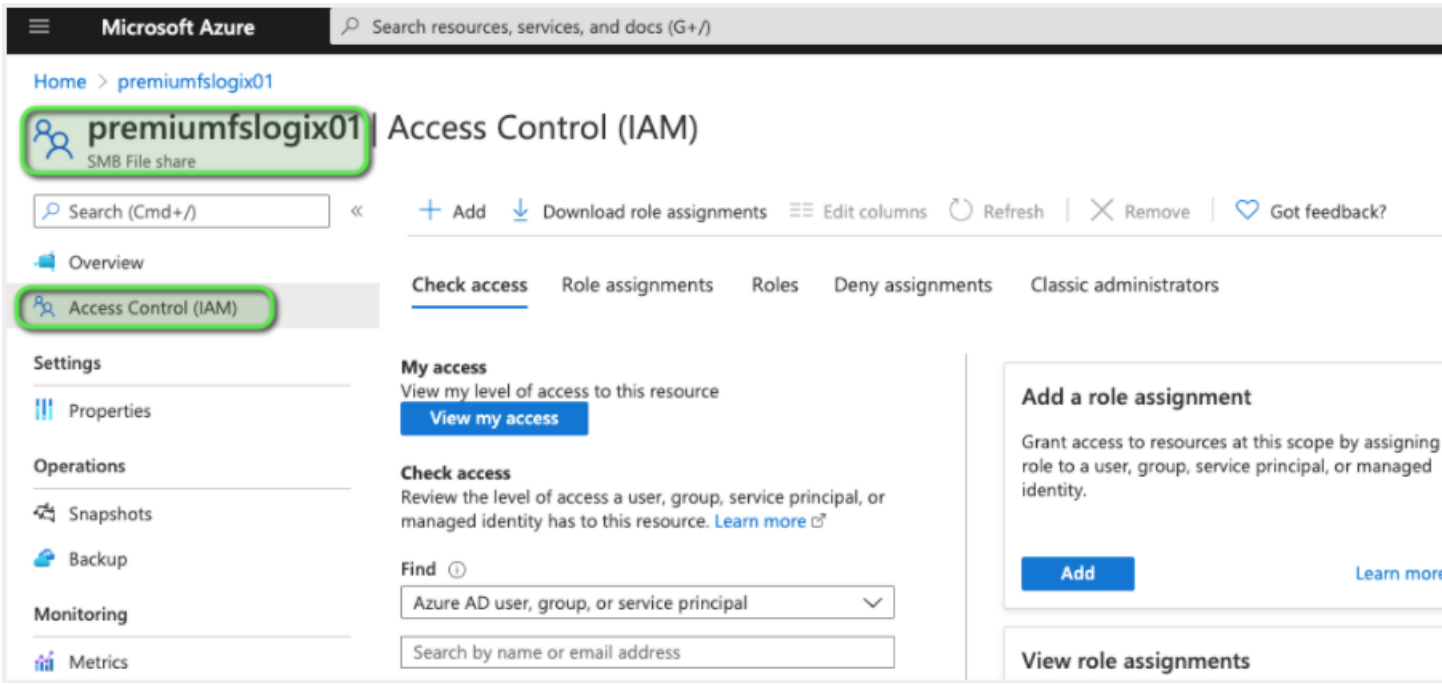
Configure Azure Files Permissions for MSIX App Attach

Nerdio Manager leverages Azure Files share technology to store MSIX 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



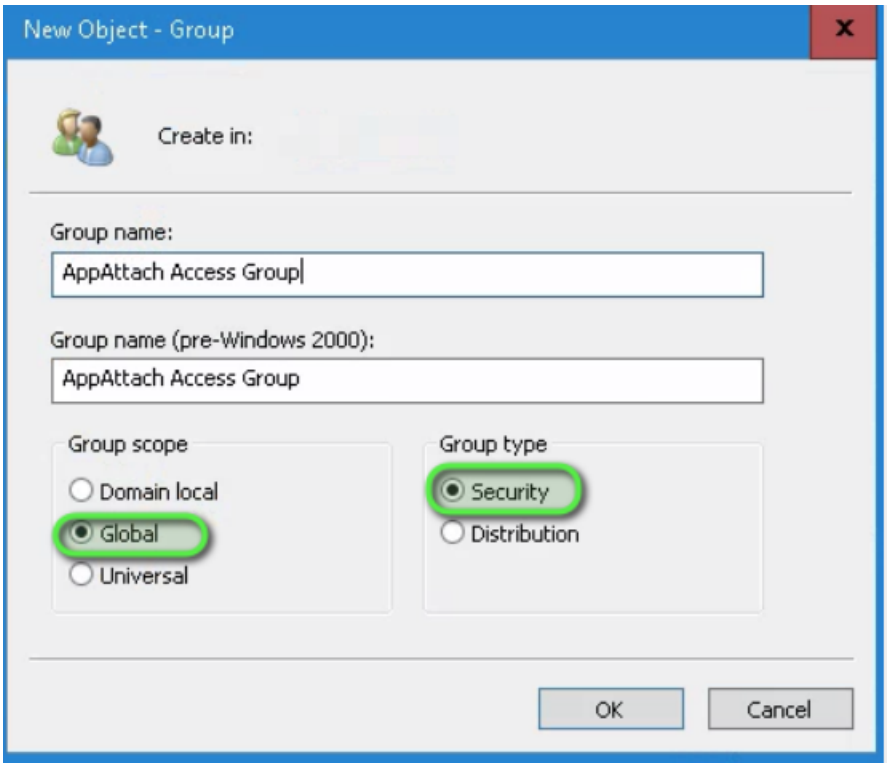
NTFS Permissions

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

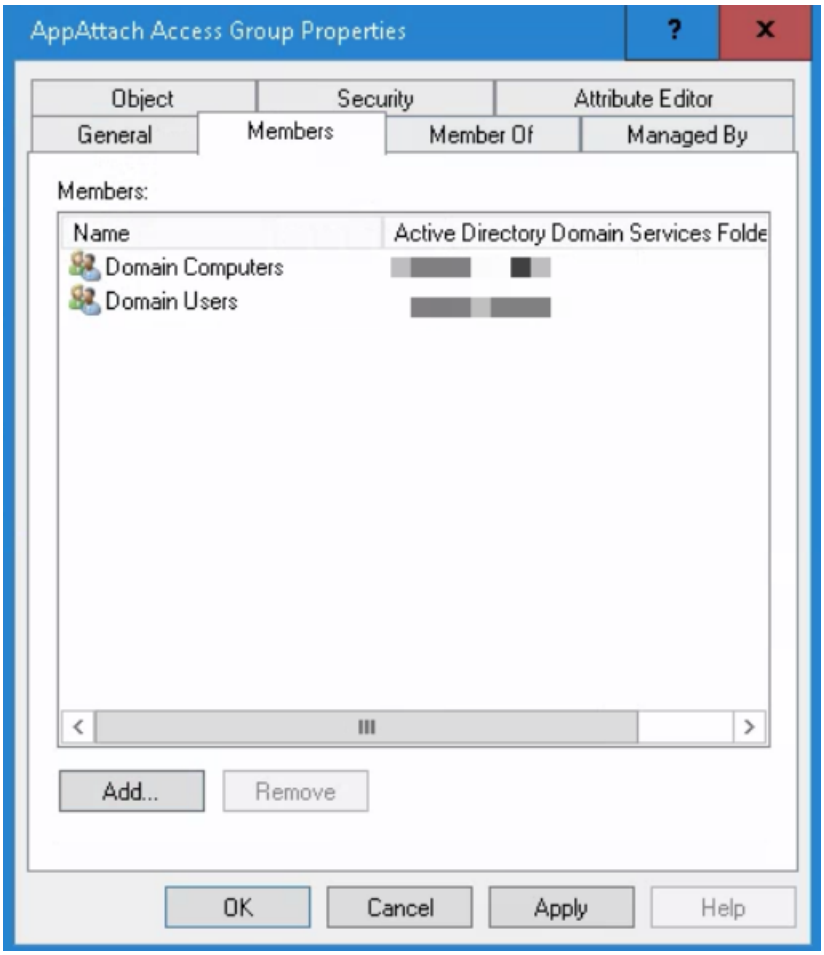
already have the necessary configuration. However, Azure Files share Access Control still needs to be configured.

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.

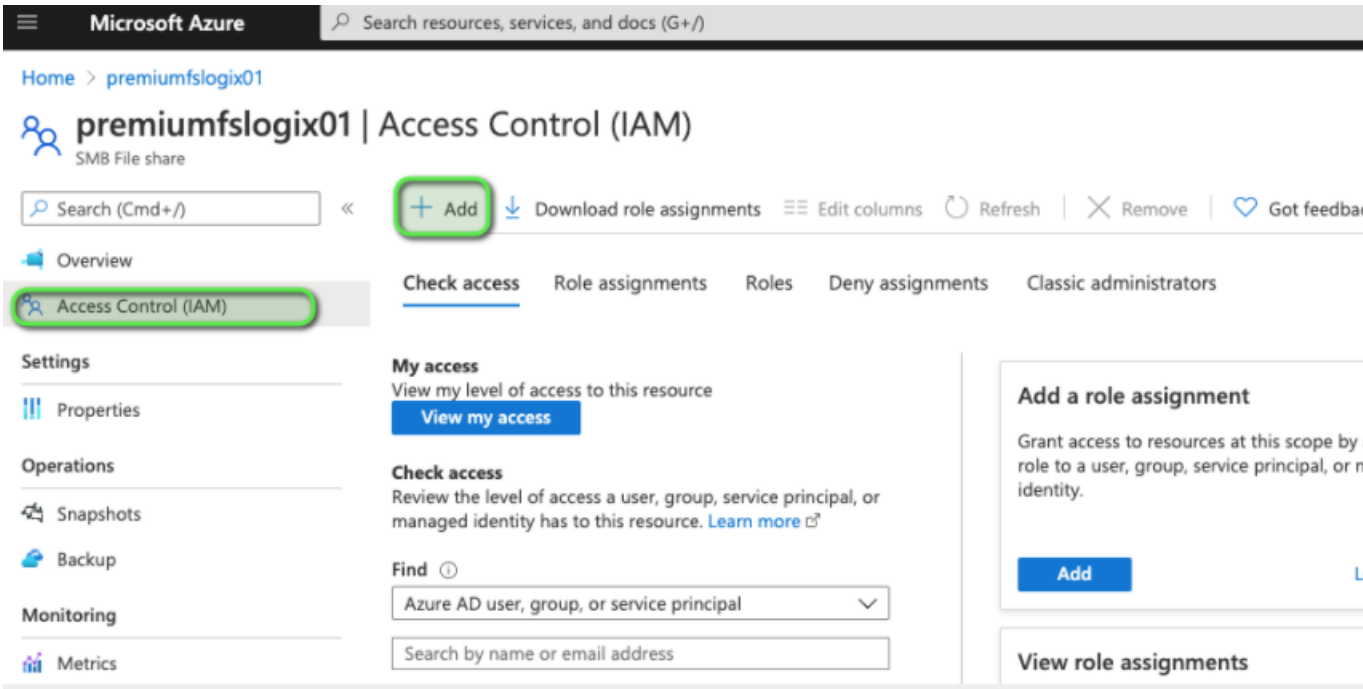


2. Add **Domain Computers** and **Domain Users** to the new group.



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 next step is to configure Role-based Access Control to Nerdio Manager.

Role-based Access Control (RBAC) in Nerdio Manager

You can use Role-based Access Controls (RBAC) to allow users in your organization to sign in to Nerdio Manager and control which actions they can perform once signed in.

The following roles are available:

- **AVD Admin**: A user with the AVD Admin role has complete access to all areas of Nerdio Manager. Only AVD Admins can manage users and roles.
- **Desktop Admin**: A user with the Desktop Admin role has complete access to user sessions, the ability to view Host Pools, power on/off/restart session hosts, but does not have the ability to add/remove hosts or change any host pool settings. This role also allows for full access to Desktop Images and Scripted Actions.
- **Help Desk**: A user with the Help Desk role has access to manage user sessions only.
- **Reviewer**: A user with the Reviewer role has view-only access to all areas of Nerdio Manager. They cannot make edits and save changes.
- **End User**: A user with the End User role can view and manage their own sessions (message, sign out, disconnect). Personal desktop users can restart, power off, and power on their personal desktops.

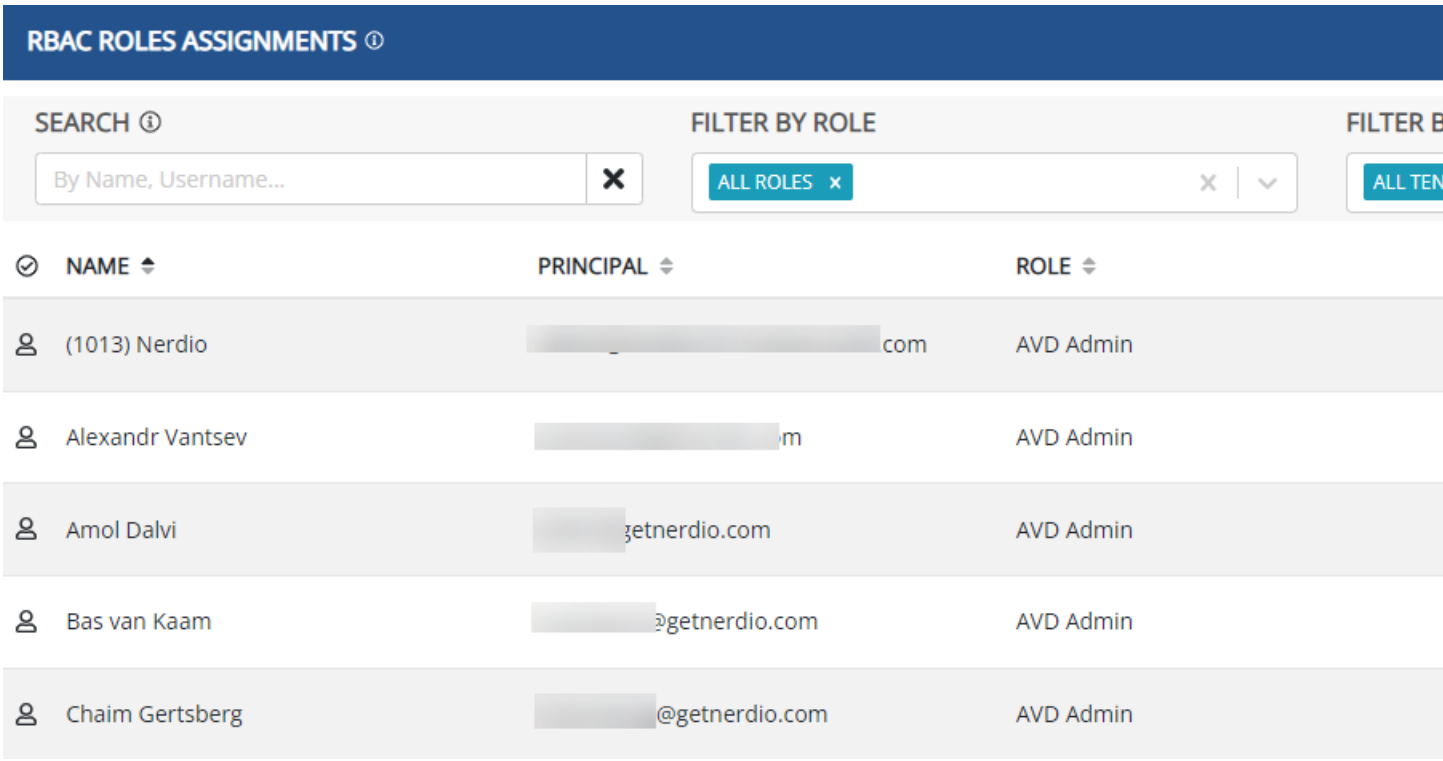
For more information about custom roles, see "Role-based Access Control (RBAC) Custom Roles" on page 204.

Companion Video

Select this link for a deep dive into RBAC.

Users and Roles Management

- Navigate to **RBAC Roles** > **Assignments**. The list of users is displayed.



Notes:

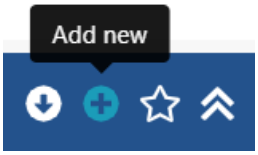
- The search section at the top allows you to search by various fields, including name, username, role, and Workspace.
- You can have the system list up to 1,000 rows on a single page. This is particularly useful when you are looking at a list of end users, which can often be hundreds or thousands.
- Select the down arrow next to **`Edit`** to display an action menu.

Add Users to Roles/Workspaces

You can add users to Roles/Workspaces.

To add users to Roles/Workspaces:

1. Navigate to **RBAC Roles** > **Assignments**.
2. In the upper right side, select the **Add new** icon or select the **Add** button.



3. Enter the following information:
    - **Role**: From the drop-down list, select a role.
    - **Users/Groups**: From the drop-down list, select the users/groups you wish to grant access to.
    - **AVD Tenant**: From the drop-down list, select the AVD tenant(s) you wish to grant access to.
    - **Workspace**: For Workspaces roles, from the drop-down list, select the Workspace(s) the user should have access to.
    - **Images**: For Desktop Images roles, from the drop-down list, select the Desktop Image(s) the user should have access to.
    - **Host Pools**: For Host Pool roles, from the drop-down list, select the Host Pools(s) the user should have access to.
4. Once you have entered all the desired information, select **OK**.

Notes:

- The changes are logged as a task. You can review the task's status to ensure the task completed successfully.
- Once access has been granted, users may sign in to Nerdio Manager using their Entra ID username and password. Simply share the URL for Nerdio Manager from your browser's address bar with the user. If MFA is being enforced, the user needs to go through the MFA process while signing in.

Edit a User's Roles/Workspaces

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

To edit a user:

1. Navigate to **RBAC Roles** > **Assignments**.
2. Locate the user you wish to edit.
3. Select **`Edit`**.
4. Once you have made the changes, select **`OK`**.

> **Note**: The changes are logged as a task. You can review the task's status to ensure the task completed successfully.

Remove User Access

You can prevent a user from accessing Nerdio Manager by removing the user's access.

To remove a user's access:

1. Navigate to **RBAC Roles** > **Assignments**.
2. Locate the user you wish to work with.
3. From the action menu, select **`Remove access`**.
4. On the confirmation window, select **`OK`**.

> **Note**: The changes are logged as a task. You can review the task's status to ensure the task completed successfully.

Role-based Access Control (RBAC) Custom Roles

You can create custom roles to control access to all areas of Nerdio Manager. Custom roles define the scope and level of access and can be assigned to users and security groups. Users

can access modules in read-only or full-access mode.

To create a custom role:

1. Navigate to **RBAC Roles** > **Definitions** .
2. Select **Add**.
3. Enter the following information:
    - **Name**: Type the custom role's name.
    - **Description**: Type a description of the custom role.
    - **Modules**: Select all the applicable modules and modes.

Module	Modes
Dashboard	• **Read Only**
Workspaces	• **Read Only** • **Full Access** • **Manage hosts**: Allow users to manage hosts within assigned host pools. • **Manage assignments**: Allow users to manage assignments within assigned host pools. • **Manage sessions**: Allow users to manage sessions within assigned host pools. • **Manage power state**: Allow users to manage the power state of the sessions within assigned host pools. • **Manage drain mode**: Allow users to manage the drain mode of the sessions within assigned host pools.

Module	Modes
	• **Run scripted actions**: Allow users to run scripted actions within assigned host pools.
Desktop Images	• **Read Only** • **Full Access**
Intune	Global Roles: • **Read Only** • **Full Access** 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** Manage Roles: • **Manage Devices** • **Manage Devices Privileged** • **Manage BitLocker**

Module	Modes
	• **Manage Antivirus** • **Manage Device Groups** • **Manage User Groups** • **Manage Locate Device** • **Manage Policies** • **Manage Applications and App Policies** • **Manage Update Rings and Policies**
Intune > Windows 365	• **Read Only** • **Full Access**
App Attach	• **Read Only** • **Full Access**
UAM > Deployment Policies	• **Read Only** • **Full Access**
UAM > App Groups	• **Read Only** • **Full Access**
UAM > Catalog	• **Read Catalog** • **Manage Catalog**: Allow users to manage UAM catalogs and performs tasks such as importing and deploying apps. • **Manage Shell App Parameters**: Allow users to manage Shell App parameters.
Scripted Actions	• **Read Only** • **Full Access**

Module	Modes
Monitoring	• **Read Only**
Storage > Azure Files	• **Read Only** • **Full Access** • **Manage Profiles**: Allow users to manage FSLogix profiles without the need for an active user session and without the need to provide full control to the file share.
Advisor > Modeler	• **Read Only** • **Full Access**
Advisor > Recommendations	• **Read Only** • **Full Access**
Advisor > Rules	• **Read Only** • **Full Access**
Storage > Azure NetApp Files	• **Read Only** • **Full Access**
Storage > Log Analytics	• **Read Only** • **Full Access**
Desktops	• **Full Access**

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

Note: From the list of definitions, you can edit or delete a custom role.

For more information, see Role-based Access Control (RBAC) in Nerdio Manager.

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 Managerinterprets 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.