

LAB GUIDE

MSP Foundations



New Customer (Greenfield)

If the customer doesn't have need for physical hardware or domain services, try [Microsoft Entra ID](#) with [Entra Join](#).



Customer has a physical domain controller already.

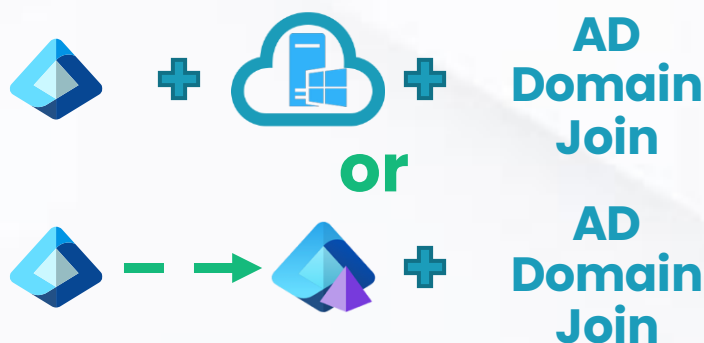
If the customer has a physical domain controller and can't / won't move away from it, use [Entra Connect](#) to create synchronization with [Microsoft Entra ID](#). You can then [hybrid Entra join](#) or use [AD domain join](#) to join virtual machines to the domain.



Customer has no infrastructure but needs a domain controller

If the customer has no physical infrastructure but needs a domain controller, try [Microsoft Entra ID](#), [Active Directory Domain Services \(VM DC\)](#), or [Microsoft Entra Domain Services](#).

If you choose Microsoft Entra Domain Services, Microsoft will create a managed virtual domain controller for you. Microsoft Entra is then used to manage users / groups / access. Your AVD machines can be joined to the domain via AD Join and physical endpoints can be directly Entra joined to Entra ID.



B-Series

Accrues credits for capacity bursting.
Use for:
Web servers, small databases, development environments.

For general computing requiring consistent CPU and low memory usage.

Use for:
Enterprise apps, app servers, medium-traffic web servers.

D-Series

E-Series

For RAM-intensive general computing.
Use for:
Database servers, RDS Session Hosts.

Offers virtual cores for CPU-intensive workloads with less of a need for RAM.

Use for:
Web servers, gaming, video encoding.

DI-Series

F-Series

Offers non-virtual cores for CPU-intensive workloads.

Use for:
Web servers, gaming, video encoding.

These series families include GPUs.

Use for:
If you need a dedicated GPU, start here!

N-Series

Azure Storage Use Cases

Standard HDD

- *For low disk I/O applications.*

Use for:

- ***Test Environments***
- ***Proxy Servers***
- ***Archived Servers***

Standard SSD

- *For non-disk I/O-heavy applications.*

Use for:

- ***Domain Controllers***
- ***File Servers***
- ***Most VDI Workloads***

Premium SSD

- *For disk I/O-intensive applications.*

Use for:

- ***Virtual Desktops***
- ***SQL Servers***
- ***Application Development***

Ultra SSD

- *For disk-intensive workloads.*

Use for:

- ***SAP HANA***
- ***Top-tier Databases***
- ***Transaction-heavy workloads***

LAB GUIDE

MSP Foundations - Day 1



Day 1 - Lab 1



Nerdio Manager allows you to create a connection between Nerdio Manager and Active Directory.

The installation process has the following workflow:

1. [Create an AD User Management Connection](#)
2. [Install the Hybrid Connection Manager \(HCM\)](#)
3. [Configure the Hybrid Connection's Credentials](#)

Notes: *There is no additional Nerdio cost to utilize AD User Management, but Service Bus Relay Hybrid Connections do have an additional Azure cost for each connection.*

Each domain controller connected to Nerdio Manager counts as a single connection.

<https://azure.microsoft.com/en-us/pricing/details/service-bus/>

App Service Plan	Hybrid Connection Limit
Basic (Nerdio Default)	5
Standard	25
Premium (v1-v3)	220
Isolated (v1-v2)	220

Day 1 – Lab 1.1 | Walkthrough

Create an AD User Management connection



1. In Nerdio Manager, at the MSP level, navigate to [Settings > AD User Management](#).

2. Select [Add](#).

3. Enter the necessary info.

- **Account:** From the drop-down list, select the account that uses this connection.
- **Hostname:** Type the fully qualified domain name for the domain controller where the hybrid connection manager will be installed. (**note** – domain controller must have internet access).
- **Port:** Type the destination port for the hybrid connection. (**note** – it is recommended that you use the default port 9389).
- **Service Bus:** From the drop-down list, select an existing service bus relay or create a new one.

A screenshot of a web-based dialog box titled "AD USER MANAGEMENT CONNECTION". It contains four input fields: "Account:" with a dropdown menu showing "Select Account..."; "Hostname:" with a text input field containing "Required"; "Port:" with a text input field containing "9389"; and "Service Bus:" with a dropdown menu showing "Type name to select existing or create new...". At the bottom right are "Cancel" and "OK" buttons.

AD USER MANAGEMENT CONNECTION

Account: ⓘ
Select Account...

Hostname: ⓘ
Required

Port: ⓘ
9389

Service Bus: ⓘ
Type name to select existing or create new...

Cancel OK

4. Click [OK](#).

Day 1 – Lab 1.2 | Walkthrough

Install the Hybrid Connection Manager



1. In Nerdio Manager, at the MSP level, navigate to [Settings > AD User Management](#).

2. Locate the AD User Management connection you wish to work with and select [continue configuration](#).

AD USER MANAGEMENT CONNECTION

Service Bus Namespace: TestRPServiceBus

Name: hybrid-1-adws

Endpoint: Nerdioadmin:9389

The Hybrid Connections feature requires a relay agent in the network that hosts your Hybrid Connection endpoint. That relay agent is called the [Hybrid Connection Manager \(HCM\)](#). See [this Microsoft doc](#) for more info.

Gateway Connection String: Endpoint=sb://testrpservicebus.servicebus.windows.net/Sh...

Close

3. Make a note of the connect information, which is needed in the next step. In addition, use the copy icon to copy the [Gateway Connection String](#) to the clipboard.

4. See this Microsoft article for full details about how to install HCM.

<https://learn.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections#hybrid-connection-manager>

Hybrid Connection Manager

About

NAME	AZURE STATUS	SERVICE NAME	ENDPOINT
Add a new Hybrid Connection			

Enter Manually

Refresh

Day 1 – Lab 1.3 | Walkthrough

Configure the Hybrid Connection's Creds



1. In Nerdio Manager, at the Account level, navigate to [Settings > Integrations](#).

2. In the [AD User Management Connection](#) tile, select [edit](#).



AD User Management Connection ⓘ
hybrid-278-adws: **Connected** [edit](#) [test](#)

3. In the [Active Directory Credentials](#) tab, enter the following information:



- Username: Type the username.
- Password: Type the password.

4. Click [Next](#).

5. In the [Organizational Unit Setup](#) tab, enter the following information:
Organizational Unit: From the list, select the Organizational Unit.

Day 1 – Lab 1.3 | Walkthrough

Configure the Hybrid Connection's Creds



6. Once you have entered all the desired information, click [Next](#).
7. In the [Default Organization Units](#) tab, enter the following information:
- Users: From the drop-down list, select the OU that is the default when new users are created.
 - Groups: From the drop-down list, select the OU that is the default when new groups are created.

AD USER MANAGEMENT CONNECTION

Active Directory Credentials

Organizational Unit Setup

Default Organizational Units

Choose the default Organizational Units new users and groups will be placed in.

USERS: ⓘ

☐ Domain Controllers

☐ Entra Synced Groups

☒ Entra Synced Users

☐ Nerdio Sales

GROUPS: ⓘ

☐ Domain Controllers

☒ Entra Synced Groups

☐ Entra Synced Users

☐ Nerdio Sales

Cancel

Save & close

8. Once you have entered all the desired information, select [Save & close](#). *Nerdio Manager attempts to make the connection. You can see the task's status in Integrations Tasks.*

Riviere Alpha

Created: Apr 29, 2023 08:26 PM

Azure tenant: riv[REDACTED].com

Subscription(s): Microsoft Azure (69[REDACTED]7c7)

Azure region(s): centralus, eastus, eastus2

Identity: Entra ID

App Registration: [REDACTED]

AD User Management Connection: **Connected**

Online, last updated: Oct 7, 2024 12:40 PM

Day 1 - Lab 2

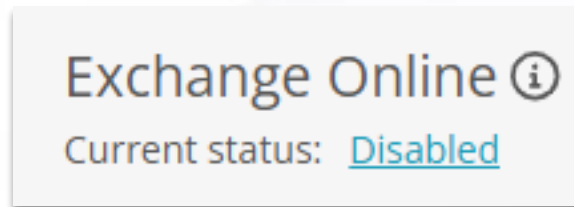


Day 1 – Lab 2.1 | Walkthrough

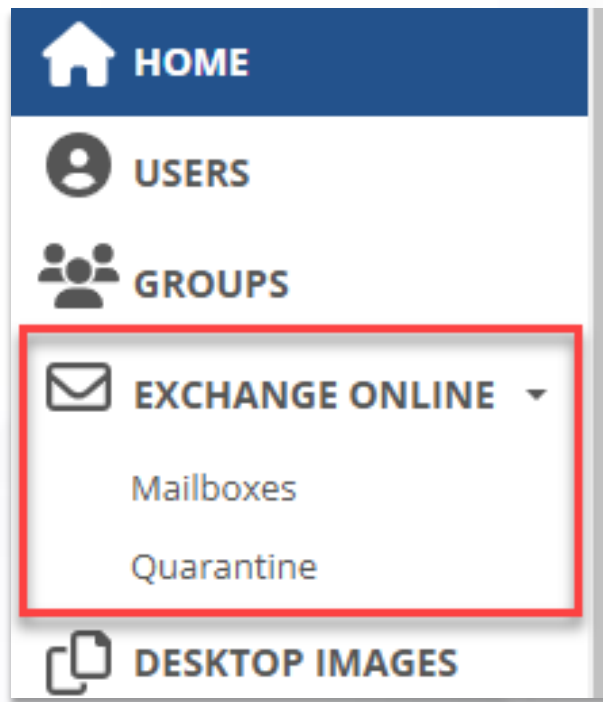
Exchange Online Management



1. At the account level, navigate to [Settings > Integration](#).
2. In the [Exchange Online](#) tile, select [Disabled](#).



3. When prompted, confirm that you want to enable. The [Exchange Online](#) menu options are now available for this account.



Day 1 – Lab 2.2 | Walkthrough

Manage Mailbox Properties



1. At the account level, navigate to [Exchange Online > Mailboxes](#).

2. Locate the mailbox you wish to work with and select [Properties](#).

The screenshot shows the 'Properties' page for a mailbox in Exchange Online. It is divided into four sections: GENERAL, DELEGATION, MAILBOX, and OTHER. Each section contains specific settings and a 'Manage' link.

Section	Property	Value	Action
GENERAL	Email addresses	testuser0@nerdioandy.onmicrosoft.com	Manage
	Type	User mailbox	Convert to Shared mailbox
	Mailbox usage	0.55 MB / 49.5 GB (0.00%)	
	Hide from global address list (GAL)	No	Edit
DELEGATION	Send as (0)		Edit
	Send on behalf of (0)		Edit
	Read and manage (Full Access) (0)		Edit
MAILBOX	Email forwarding	No forwarding options set currently	Manage
OTHER	Automatic replies	Disabled	Manage
	Mailbox archive	None	Manage
	Litigation hold	Disabled	Manage

3. Manage the following properties:

Email addresses: Select Manage to edit the current email address. In addition, you can add, edit, and delete additional email addresses.

Type: Select Convert to Shared mailbox to convert the mailbox from a regular to a shared mailbox.

Hide from global address list (GAL): Select Edit to toggle this option On/Off.

Delegation: Send as, Send on behalf of, read and manage.

Email forwarding: Select Manage to configure the email forwarding for this mailbox.

Other: Automatic replies: Select Manage to configure the automatic replies for this mailbox.

Other: Mailbox archive: Select Manage to configure the mailbox archive for this mailbox.

Other: Litigation hold: Select Manage to configure the litigation hold for this mailbox.

Day 1 – Lab 9.3 | Walkthrough

Manage Exchange Online Quarantine



1. At the account level, navigate to [Exchange Online > Quarantine](#).

QUARANTINE									
TIME RECEIVED	SUBJECT	SENDER	QUARANTINE REASON	RELEASE STATUS	POLICY TYPE	EXPIRES	RECIPIENT		
Nov 4, 2024 10:19:15 AM	TEST for Quarantine	kirc...@om	File Type Block	Needs review	Anti-malware policy	Dec 4, 2024 10:19 AM	nite...	foxt...	Release
1 item									

2. Locate the quarantined item you wish to work with and select [Release](#).

RELEASE EMAIL

Release email to recipients inboxes

☐ Release to all recipients

☒ Release to one or more of the original recipients of the email

Select... | v

☒ Send a copy of this message to other recipients ⓘ

Type user name | v

CancelRelease

3. Enter the following information:

- **Release email to recipients' inboxes:** Select the desired option to release to all recipients or selected recipients.
- **Send a copy of this message to other recipients:** Select this option, and select the recipients, to send a copy to other recipients.

4. Select [Release](#).

Day 1 - Lab 3

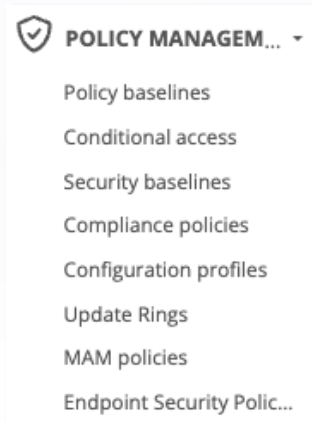


Day 1 - Lab 3.1 | Walkthrough

Importing Intune Policies



1. Expand the [Policy Management blade](#) and select the policy type you'd like to import. (MSP / Global level).



2. Click [Import](#) and select a policy from a list of your custom Intune policies.

- We recommend tagging policies for ease of management.



3. Add a changelog description and click [Import](#) to finish.

Note: Turn on [Evaluate user/group assignments](#) for policies that are already assigned to endpoints.

IMPORT INTUNE CONFIGURATION PROFILE AS OF JUL 10, 2024 03:43:03 PM

MSP Search by Name...

AVAILABLE POLICY	PLATFORM	LAST MODIFIED
<input checked="" type="radio"/> Atlanta Config Profile	Windows 10 and later	Apr 11, 2024 02:04 PM
<input type="radio"/> Atlanta Config Profile	Windows 10 and later	Jul 10, 2024 11:38 AM
<input type="radio"/> Kansas City Intune Policy	Windows 10 and later	Mar 14, 2024 03:26 PM
<input type="radio"/> KansasCityWallpaper	Windows 10 and later	Mar 14, 2024 03:35 PM
<input type="radio"/> LA Win11 Config Profile	Windows 10 and later	May 9, 2024 05:46 PM
<input type="radio"/> LA Win11 Config Profile	Windows 10 and later	May 9, 2024 05:44 PM
<input type="radio"/> MSP MSP TC	Windows 10 and later	May 23, 2024 03:31 PM
<input type="radio"/> MSP MSP TC	Windows 10 and later	May 23, 2024 04:11 PM
<input type="radio"/> MSP TC Wallpaper	Windows 10 and later	May 23, 2024 04:11 PM
<input type="radio"/> MSP TC Wallpaper	Windows 10 and later	Feb 21, 2024 01:09 PM

Tags: Windows x User Experience x x v

Changelog: *

Initial Import

☒ Evaluate user/group assignments o

Cancel Import

Day 1 – Lab 3.2 | Walkthrough

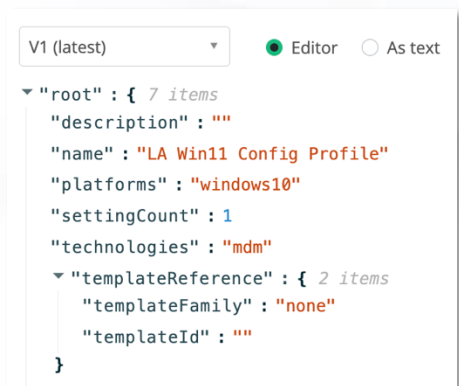


Editing Policies in Nerdio

1. Click the [dropdown menu](#) next to [assign](#) to modify an imported or cloned policy.
 - *Nerdio default policies cannot be edited and must be cloned.*
2. Click Edit to modify the policy.
3. Use the Name tab to update the policy name, description and tags, then click [Next](#).

4. Use the settings tab to modify the policy JSON, then click [Next](#).

- Use the dropdown menu to select the version to modify.
- Use the radio buttons to toggle between editing JSON in text or via the editor.



5. Enter information into the [Changelog](#) and then click [Save & Close](#) to finish.
 - Select **Create a new version** if you are changing functionality in the policy.
 - Select **Edit the latest existing version** if you are resolving a typo or an issue within the version.

☒ Create a new version

☐ Edit the latest existing version

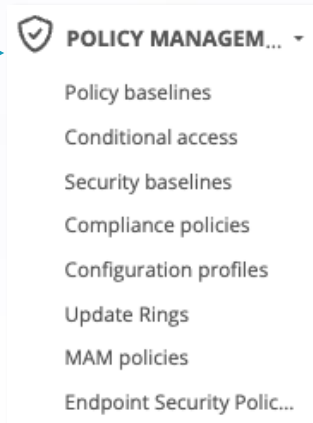
Initial Import

Note: Only custom policies can be edited or changed. To change NMM policies, clone them first and then modify the cloned version.

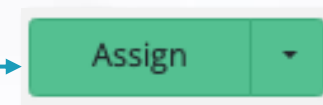
Day 1 – Lab 3.3 | Walkthrough

Assigning Policies in NMM

1. Expand the [Policy Management blade](#) and click the policy type you'd like to assign (MSP / Global level).



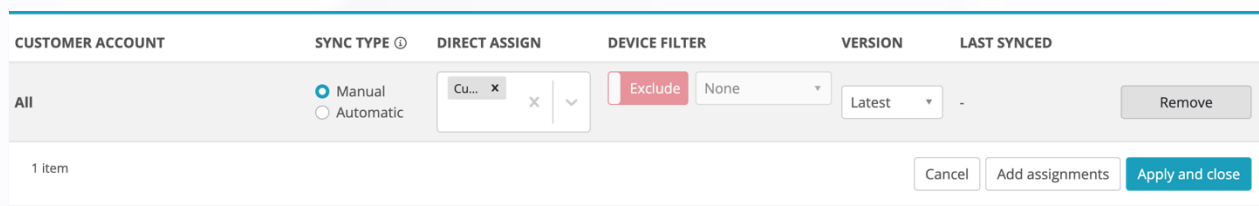
2. Find the target policy and click [Assign](#) then [Add Assignment](#).



3. Use the [dropdown menu](#) to select the account(s) to assign the policy to.

Selecting Add will add the policy to any new accounts selected without modifying the original assigned list (if applicable).

Selecting Overwrite will remove any original assignments and assign the policy to the accounts you've defined in this menu.



4. When you're finished, click [Confirm](#) then [Apply and Close](#).

Day 1 – Lab 3.3 | Walkthrough

Assigning Policies in NMM



5. Once you've added the assignments, select your [Sync Type](#):

- **Automatic** will automatically cascade any changes made to the policy to the customer accounts you've assigned it to, keeping everything aligned.
- If you set the sync type to **Manual**, you'll need to return to this page to update versions and apply them to push updates to the customer account level.

6. Select the [Version](#) you want to assign

- Selecting **Latest** will apply the latest version to the account when it is synced.
- Selecting a **Specific Version** will only assign the selected version, it will not automatically change as new versions become available.

The screenshot shows a table with columns: CUSTOMER ACCOUNT, SYNC TYPE, DIRECT ASSIGN, DEVICE FILTER, VERSION, and LAST SYNCED. The first row has 'All' under CUSTOMER ACCOUNT, 'Manual' selected under SYNC TYPE, 'Cu...' under DIRECT ASSIGN, 'Exclude' under DEVICE FILTER, 'Latest' under VERSION, and '-' under LAST SYNCED. At the bottom, there are buttons for 'Cancel', 'Add assignments', and 'Apply and close'.

7. When you're finished making your selections, click [Apply and Close](#) to commit your changes.

Granular policy assignment allows for applying specific settings to targeted users, groups, or devices.

You will have tailored policy management to meet specific client needs. As well as more efficient operations through precise control over policies.

This is the view when assigning policies. You can now see [Direct Assign](#) and [Device Filter](#) after you add the assignment and before applying and saving.

The screenshot shows a table titled 'ASSIGNMENTS - NMM AUTO SUBSCRIBE FOR REMOTE DESKTOP & AVD'. It has columns: CUSTOMER ACCOUNT, SYNC TYPE, DIRECT ASSIGN, DEVICE FILTER, VERSION, and LAST SYNCED. There are two rows. The first row is for '(7) Ganar Hart, Inc.' with 'Automatic' sync type, 'All Devices' under DIRECT ASSIGN, 'Exclude' under DEVICE FILTER, 'Latest(v1)' under VERSION, and 'Nov 7, 2023 11:55:35 AM' under LAST SYNCED. The second row is for '(1) Nube Hart, Inc.' with 'Automatic' sync type, 'All Devices' under DIRECT ASSIGN, 'Exclude' under DEVICE FILTER, 'Latest(v1)' under VERSION, and 'Oct 12, 2023 01:17:13 PM' under LAST SYNCED. At the bottom, there are buttons for 'Cancel', 'Add assignments', and 'Apply and close'.

Day 1 – Lab 3.4 | Walkthrough

Group Templates



Group templates allow you to directly assign policies at the MSP level to users and devices that belong to a group that is defined in the group template.

For example, you can create a group template for all Microsoft devices that are not personally owned. This gives you additional flexibility when assigning policies.

Once you create your group templates, they may be used for policy assignments at the MSP level.

The following “purpose types” are available:

- **None:** Use this for any kind of dynamic group you’d like to create
- **Policy Management:** Use this for managing policy assignment.
- **License Management:** Use this for managing Microsoft license assignment.

CREATE GROUP TEMPLATE

General

Name Template

NAME

PURPOSE TYPE

MEMBERSHIP TYPE

None

None

Policy Management

License Management

Close

Next

Day 1 – Lab 3.4 | Walkthrough

Group Templates



The following template membership types are available:

- **Assigned:** Select this type to include any user and/or device assigned to any group
- **Dynamic Device:** Select this option to include all devices or specific devices.
- **Dynamic User:** Select this option to include all users or specific users.

MEMBERSHIP TYPE Dynamic Device ▼

DYNAMIC RULE New

And/Or	Property	Operator	Value
▼	device... ▼	Equals ▼	Microsoft
And ▼	deviceO... ▼	Not Equ... ▼	Personal

MEMBERSHIP TYPE Dynamic User ▼

DYNAMIC RULE Predefined All users ▼

DYNAMIC RULE New

And/Or	Property	Operator	Value
▼	city ▼	Equals ▼	New York
And ▼	depart... ▼	Equals ▼	HR

Day 1 – Lab 3.5 | Walkthrough

Create a Group Template



1. At the MSP level, navigate to [Group Templates](#).

2. Select [add new group template](#).

3. In the General tab, enter the follow information.

- **Name:** Type the group template name.
- **Purpose Type:** From the drop-down list, select the purpose.
- **Membership Type:** From the drop-down list, select the membership type, as described above.
- **Dynamic Rule:** For Dynamic User or Dynamic Device, build the dynamic rule, as described above.

CREATE GROUP TEMPLATE

General

Name Template

NAME

MEMBERSHIP TYPE

Dynamic Device

DYNAMIC RULE

New

And/Or

Property

objectId

Operator

Not Equ...

Value

null

Add expression

Note: Select [Add expression to add more to the rule](#).

4. In [Name Template](#) tab, enter the following information to generate a unique group name per policy.

Guide: How to create templates

Required parameters (you need to use at least one of these):

- `{ $policyname }`
- `{ $policyid }`

Optional parameters:

- `{ $customername }`
- `{ $type }`
- `{ $version }`

You can restrict max number of characters to avoid running into limitations:
For example, `{ $policyname:4 }` would only use the first 4 characters from the policy name.

Some examples (click to add to template):

- `{ $customername:5 }- { $policyname:12 }- { $version }`
- `{ $customername:5 }- { $policyname:12 }- { $version }`
- `SG- { $policyname:20 }`
- `SG- { $policyid }`
- `SG- { $policyid }- { $version }`

PREVIEW

NAME TEMPLATE

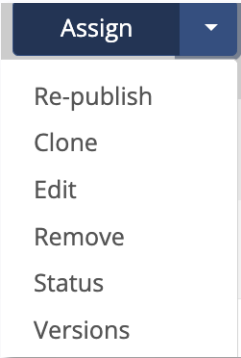
Cancel Save & close

5. Select [Save & close](#) when finished.

Review the Changelog

Use the change log to document and review policy changes.

1. Find the policy you'd like to review and use the [dropdown menu](#) to click [Versions](#).



Check Policy Statuses

Check the status to track endpoint compliance from a single pane of glass.

1. Find the policy and use the [dropdown menu](#) to click [status](#).
- Use the [Update](#) button to update to more recent versions at the customer account level.
 - Use the [Fix Drift](#) button to resolve detected drift issues.
 - Use [Rollback](#) to swap to a previous version.

CONFIGURATION DRIFT - LAB1					As of Jul 9, 2024 10:37:51 AM
CUSTOMER ACCOUNT	SYNC TYPE	ASSIGNED VERSION	SYNC STATUS	ASSIGNED	
(1) Nube Hart, Inc.	Manual	Latest (v2)	v1 found, v2 expected	No assignments	Update
1 item					Back

Update, Rollback Policy Versions

Check the status to track endpoint compliance from a single pane of glass.

1. Find the policy and use the [dropdown menu](#) to click [status](#).

Day 1 - Lab 4



1. In Nerdio Manager, at the MSP level, navigate to [Recovery Services](#).

2. Click [Create Restore Point](#).

3. Choose your retention settings and add a description.

ADD NEW RESTORE POINT

Do you want to create a restore point?

Retention in days:

30

Description:

Enter description

With the schedule set to OFF action will be performed immediately. With schedule turned ON, the task will be performed according to the specified schedule.

SCHEDULE

Off ⓘ

Cancel

OK

4. Move the [SCHEDULE](#) slider over to on and choose when you would like these snapshots to happen.

SCHEDULE

On ⓘ

Start date:

04/30/2025 ⓘ

Time zone:

(UTC-07:00) Arizona ⓘ

Start time:

12 a.m. ⓘ

:

00 ⓘ

Repeat:

Never ⓘ

Cancel

OK

5. Click [OK](#) and the snapshots will run on that schedule.

You will be able to check your snapshots, what policies, baselines, profiles, etc are being backed up each time. As well as delete, changed, and new items from day to day,

Day 1 - Lab 5



Day 1 – Lab 5.1 | Walkthrough

Configuring Intune Policy Baselines



1. Expand the [Policy Management blade](#) and click [Policy Baselines](#) (MSP / Global level).



2. Click [Add Baseline](#).



3. Configure the following:

- A clear name for the baseline.
- A description of its function.
- Tags for ease of management.

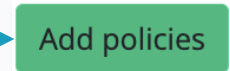
4. When you're finished, click [Save](#).



5. Once saved, click the [Policy Count](#) to add policies.

NAME ⓘ	POLICY COUNT ⓘ
Windows 11 Device configuration policy baseline for Windows 11 machines.	2

5. Click [Add Policies](#) to add policies to the baseline. Then click [Apply and Close](#).



Day 1 – Lab 5.1 | Walkthrough

Configuring Intune Policy Baselines



6. Arrange the policy baselines in order of priority. The weight of priority is from the top-down.

7. Click [Assign](#) and [Add Assignments](#).

8. Choose the baseline behavior.

- Enforced baselines apply to and configure endpoints.
- Report-only track drift and changes on endpoints.

9. Choose to add or overwrite the assignments.

- Adding assignments will add new entries to the existing list of assigned accounts.
- Selecting overwrite will overwrite the list of currently assigned accounts.

BASELINE ASSIGNMENTS - WINDOWS 11

Select assignments.

All x [dropdown arrow]

☒ Enforced ⓘ ☐ Report-only ⓘ

☒ Add ⓘ ☐ Overwrite ⓘ

Cancel Confirm

10. When you're finished, click [Confirm](#).



ASSIGNMENTS - WINDOWS 11			
CUSTOMER ACCOUNT	MODE ⓘ	POLICIES COUNT ⓘ	LAST SYNCED
All	Enforced	2	-
1 item			
Cancel Add assignments Apply and close			

11. Then click [Apply and Close](#) to assign the baseline to the selected accounts.

Day 1 – Lab 5.2 | Walkthrough

Assigning Policies to Endpoints



1. From the customer account level, go to [Policy Management](#) and select the policy type you'd like to assign.

2. Locate the policy you'd like to deploy and click [Assign](#).

3. Select an option for assignment.

- Using Included Groups will allow you to select groups to assign the policy to.
- Or, you can select all users and / or all devices and use exclusions.

4. Once assigned, your

- Using [Included Groups](#) will allow you to select groups to assign the policy to.
- Or you can select [all users](#) and / or [all devices](#) and use exclusions.

POLICY DETAILS - ATLANTA CONFIG PROFILE

ASSIGNMENTS:

Included Groups



☒ All users ⓘ ☒ All devices ⓘ

Excluded Groups

Nerdio Presenters (nerdiopresenters@nerdiouniversity.com) x

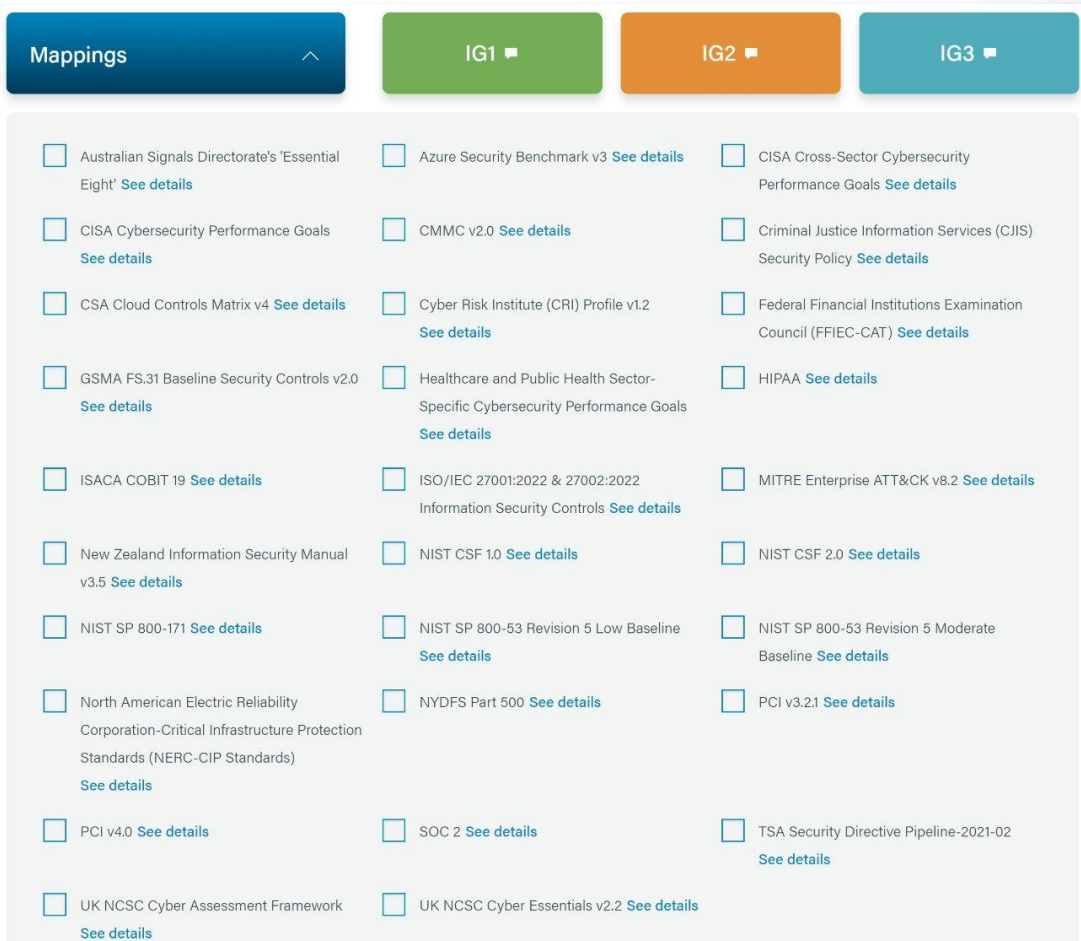


Cancel

Confirm

Pre-configured templates that align with CIS standards and automatic updates that keep policies CIS-compliant.

- Pre-configured for easy CIS-compliant deployment.
- Ensure consistency and reduce manual effort with centralized control.
- Keep policies CIS-compliant with automatic updates



Day 1 – Lab 5.3 | Walkthrough

CIS Baselines



1. Navigate to [Policy Management](#), at the MSP level, and choose [CIS Policy baselines](#).

Note: The policies are already built for Windows 10 & 11, CIS Level 1.

CIS POLICY BASELINES				
<div>Last Modified</div> <div><div></div><div>24 hours</div><div>30 days</div><div>All</div></div>		<div>Search by name, id...</div>		
		<div>FILTER BY TAGS</div> <div>All</div>		
NAME	POLICY COUNT	TAGS	ASSIGNMENTS	LAST MODIFIED
<div>CIS Windows 10 Level 1 v3.0.1</div>	12	Windows10	Nube Hart, Inc. (1) Enforced Ganar Hart, Inc. (7) Enforced	Nov 7, 2024 04:48 AM
<div>CIS Windows 11 Level 1 v3.0.1</div>	13	Windows11	Nube Hart, Inc. (1) Enforced Nerdio Andy (278) Enforced Nerdio Andy (280) Enforced	Nov 7, 2024 09:32 AM

2. Click [Assign](#), [Add Assignments](#), and then fill out the information listed below.

BASELINE ASSIGNMENTS - CIS WINDOWS 10 LEVEL 1 V3.0.1

Select assignments.

Select...

☐ Enforced

☒ Report-only

☒ Add

☐ Overwrite

Cancel

Confirm

3. Click [Confirm and then Apply and close](#).

Day 1 - Lab 6



Day 1 – Lab 6.1 | Walkthrough

Configure Solution Baselines



1. In Nerdio Manager, at the MSP level, navigate to [Solution Baselines](#).
2. Locate the [Solution Baseline](#) you wish to work with.
3. From the action menu, select [Configure baseline](#).
4. In the [Prerequisites](#) tab, enter the needed information.

SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT

Prerequisites Integrations Device onboarding Notifications Summary

Name and Description

Solution Baseline for Defender for Endpoint

This Solution Baseline allows to compose a set of best practices for Microsoft Defender for Endpoint (P1 & P2) and Defender for Business. The Solution Baseline will be used as a desired state to track drift in customer environments or to force customer configuration to align with the desired state.

License validation Enforce Report-only Exclude

In order to enable the Defender for Business/Endpoint features on this customer account, the customer needs at least one supported license. Choose whether to include or exclude license validation.

Permissions Enforce Report-only Exclude

Nerdio Manager for MSP needs the appropriate permissions to access security related data from this customer account. As part of the baseline, validate if the required permissions are available.

5. In the [Integrations](#) tab, enter the needed information.

SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT

Prerequisites Integrations **Device onboarding** Notifications Summary

Device Onboarding Enforce Report-only Exclude

⚠ There is no attached policy. Canned policy "" not found. Settings will be applied. **Coming soon!**

Device onboarding profile for Intune managed devices
Deploy a configuration profile for auto enrollment of Intune managed devices.

Assignment
☒ All Devices ☐ Custom

Baseline Endpoint Security Policies
Deploy and apply the Nerdio Manager for MSP Defender for Business & Endpoint baseline policies and assign them to all devices.

Policy Baseline
☒ Policy baseline for Defender for Endpoint ☐ Custom

Assignment
☒ All devices ☐ Custom (manually assign the configuration profile)

7. In the [Summary](#) tab, review the changes.

SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT

Prerequisites Integrations Device onboarding Notifications **Summary**

Summary Enforce Report-only Exclude

Components	
Prerequisites	3
Integrations	3 1
Device onboarding	2
Notifications	1

Total

Components enabled as part of the MSP baseline 6 4

Options

☐ Process the Solution Baseline for Defender for Endpoint after saving ⓘ

☐ Do you want to remove policies that are affected by this change? ⓘ

8. Set the following options:

- Process the Solution Baseline for Endpoint after saving: Select this option to apply the solution baseline to the assigned accounts.
- Do you want to remove policies that are affected by this change?: If this option is selected, policies from this solution baseline are removed from the tenant if they don't have any other assignments.

9. Once reviewed, select [Save & close](#).

Note: Some baselines may have a different tab order.

Day 1 – Lab 6.2 | Walkthrough

Assign Accounts to a Solution Baseline



- 1. In Nerdio Manager, at the MSP level, navigate to [Solution Baselines](#).
- 2. Locate the [Solution Baseline](#) you wish to work with.
- 3. From the action menu, select [Assign](#).

ASSIGNMENTS - SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT			
CUSTOMER ACCOUNT	MODE	LAST SYNCED	
(1) Nube Hart, Inc.	<input checked="" type="radio"/> Enforce <input type="radio"/> Report-only	Feb 1, 2024 05:30:10 PM	<button>Remove</button>
1 item			
<div><button>Back</button> <button>Add assignments</button> <button>Apply and close</button></div>			

4. Select [Add assignments](#).



SOLUTION BASELINE ASSIGNMENTS - SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT

Select assignments.

Select...

☒ Add
☐ Overwrite

Cancel

Confirm

5. Enter the following information:

- **Assignments:** From the drop-down list, select the account(s) to assign.
- **Add / Overwrite:** Select whether to add the selected accounts to the existing assignments or replace (overwrite) the existing assignments with the new selections.
- Optionally, select **Remove** to remove an assignment.

6. Review and click [Confirm](#).



APPLY CHANGES - SOLUTION BASELINE FOR DEFENDER FOR ENDPOINT

Are you sure you want to apply the following changes and assign this solution baseline to selected accounts?

SOLUTION BASELINE	ACCOUNT	ACTION
Solution Baseline for Defender for Endpoint	(7) Ganar Hart, Inc.	Assign

☐ Enforce

Cancel

Confirm

7. When you are done with all changes, select [Apply and close](#).



Back

Add assignments

Apply and close

1. In Nerdio Manager, at the MSP level, navigate to [Solution Baselines](#).
2. Locate the [Solution Baseline](#) you wish to work with.

3. From the action menu, select [Status overview](#).

4. The status page uses the following colors:

- **Green:** Valid (Satisfied)
- **Yellow:** Mismatch (Drifted)
- **Red:** Not Found (Drifted)
- **Gray:** Excluded


Solution Baseline for Defender for Endpoint

DefenderForEndpoint (built-in)

Customer Compliance ⓘ

2


2



Last Modified on Jul 9, 2024 12:04 PM

Assign

▼

STATUS - SOLUTION BASELINE FOR INTUNE					As of Sep 18, 2024 07:49:02	
CUSTOMER	MODE	STATUS 			BASILINE SETTINGS	
(91) Nerdio Golf Inc.	Enforced	<div><div>5</div></div>	<div><div>3 (+4)</div></div>	<div><div>4 (+4)</div></div>	<div><div>1</div></div>	View details
(1) Nube Hart, Inc.	Enforced	<div><div>11</div></div>	<div><div>4 (+2)</div></div>	<div><div>1 (+2)</div></div>	<div><div>1</div></div>	View details
(7) Ganar Hart, Inc.	Enforced	<div><div>15</div></div>	<div><div>4</div></div>	<div><div>1</div></div>	<div><div>1</div></div>	View details

5. Optionally select [View details](#).

Baseline Settings

Filter By Result ☐ All ☐ Satisfied ☒ Drifted

SETTINGS ↕	MODE ↕	RESULT ↕	ACTUAL STATE	DESIRED STATE	
Allow BYOD	Enforced	Unavailable	State is unavailable	Disabled	Accept Drift
Allow Windows enrollment	Enforced	Unavailable	State is unavailable	Enabled	Accept Drift
Delete devices based on last check-in date	Report-only	Unavailable	State is unavailable	Disabled	Accept Drift
Deploy basic Enrollment Status Page	Report-only	Unavailable	State is unavailable	Enabled	Accept Drift
Deploy Entra Joined Standard User profile	Enforced	Mismatch	Status: Mismatch Assignment: Mismatch	Status: Valid Assignment: Custom	Accept Drift
Enable WUFB Reports	Enforced	Unavailable	State is unavailable	Enabled	Accept Drift
Endpoint reporting profile for Intune managed devices	Enforced	Mismatch	Status: Mismatch Assignment: Mismatch	Status: Valid Assignment: Custom	Accept Drift
Intune features	Report-only	Mismatch	Disabled	Enabled	Accept Drift
LAPS policy for Intune managed endpoints	Enforced	Mismatch	Status: Mismatch Assignment: Mismatch	Status: Valid Assignment: Custom	Accept Drift
Mark devices noncompliant if no compliance policy is assigned	Enforced	Unavailable	State is unavailable	Disabled	Accept Drift

Day 1 – Lab 6.3 | Walkthrough

View the status of Solution Baselines



6. For any drifted setting, select [Accept Drift](#).

7. Enter the following information:

- **Drift acceptance expires after:** From the drop-down list, select the drift expiration. Alternatively, type a date.
- **Description:** Optionally, type a description about why this drift was accepted.
- **Allow processing:** Select this option for the next republishing to try to sync the policy.

ACCEPT DRIFT FOR SOLUTION BASELINE

BASELINE:

Solution Baseline for Intune

ACTION:

Endpoint reporting profile for Intune managed devices

ACCOUNT:

Nerdio Golf Inc. (91)

Drift acceptance expires after

30 days

Oct 18, 2024

Description

Optionally, provide a description why this drift is accepted

☐ Allow processing ⓘ

Cancel

Accept

8. Once you have entered the desired information, select [Accept](#).

9. Hover over [Accepted drift](#) to see its details.

Deploy basic Enrollment status page	Report only	Unavailable	State is unavailable
Deploy Entra Joined Standard User profile	Enforced	Accepted drift	Status: Mismatch Assignment: Mismatch
Enable WUfB Reports	Enforced	Accepted drift	State is unavailable
Endpoint reporting profile for Intune managed devices	Enforced	Accepted drift	Status: Mismatch Assignment: Mismatch

Drift: Mismatch

Accepted at: Sep 18, 2024 07:53 PM

Accepted by: sl

Expires at: Oct 18, 2024 07:52 PM

Re-publishing mode: Skip processing

Description: The drift is expected and not an issue.

Day 1 - Lab 7



Day 1 – Lab 7 | Walkthrough

Tenant Monitoring



1. At the MSP-level, navigate to [Tenant Monitoring](#).
2. Select [Add Report](#).
3. In the [Report Sources](#) tab, enter the following information:
 - **Report name:** Type the report name.
 - **Report description:** Type the report description.
 - **Solution baselines:** From the drop-down list, select the solution baseline(s) to include in the report.
 - **Policy baselines:** From the drop-down list, select the policy baseline(s) to include in the report.
 - **Global policies:** Select Select to select the global policies to include in the report.

TENANT MONITORING REPORT OCTOBER 17, 2024 AT 2 PM

Report sources Report options Schedule Report confirmation

Select one or more configuration sources to compare:

- For Policies, every containing setting will be compared
- For Policy Baselines, every setting from every policy will be compared
- For Solution Baselines, all tenant-level settings and also all Policies and Policy Baselines they contain will be added to the list and compared.

Name and Description

Tenant monitoring report October 17, 2024 at 2 PM ✎

<no value> ✎

Solution baselines

Solution Baseline for Intune ✕ Solution Baseline for Intuneconnected56 ✕ ✕ | ▼ ⓘ

Policy baselines

6 - test republish ✕ ✕ | ▼ ⓘ

Global policies

4 - admin - 72 ✕ ✕ **Select** ⓘ

4. In the [Report options tab](#), enter the following:

Select report type

- From the drop-down list, select the report type.

Note:

- Select **Base** to configure the report for existing account(s).
- Select **Prospect** to configure the report for a prospect account.

Select target accounts:

- For a Base report, from the drop-down list, select the existing account(s) to include in the report.
- For a Prospect report, select +Add and follow the prompts to sign in to the customer tenant.

AUTHORIZE

Sign in to the customer tenant with an account that has read permissions for all Intune data. When you click the Sign In button, you will be redirected to the Entra ID Sign In page.

Cancel

Login

- Ignore policy names: Select this option to ignore policy names.
- Hide the actual values for settings: Select this option to hide the actual values for the settings on the report.

5. In the [Schedule](#) tab, enter the following:

Schedule: Optionally, toggle On this option and enter the desired schedule.

TENANT MONITORING REPORT OCTOBER 17, 2024 AT 2 PM

Report sources Report options **Schedule** Report confirmation

With the schedule set to OFF report will be reprocessed immediately if needed. With schedule turned ON, the reprocess task will be performed according to the specified schedule.

An existing schedule is currently active. You can edit the current schedule or delete it.

SCHEDULE On

Start date: 10/23/2024

Time zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Start time: 4 p.m. : 05

Repeat: Monthly

Day of week: Fourth Thursday

6. In the [Report Confirmation](#) tab, review the report configuration and enter the following information.

Reprocess report: Select this option reprocess the report.

7. When finished, click [Save & Close](#).

Day 1 - Lab 8



Day 1 – Lab 8 | Walkthrough

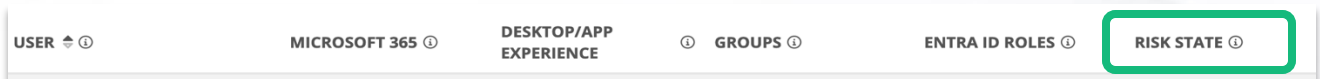
Risky Users



1. Navigate to your customer account and click on the [Users](#) blade.

2. Find a user and check the [RISK STATE](#) column.

- You can also filter different user states at the top of the page



Reduce security risks.

Ensure compliance with security protocols.

Provide safer and more efficient client accounts.

Day 1 - Lab 9



Day 1 – Lab 9 | Walkthrough

Vulnerability Dashboard



Nerdio Manager provides an MSP-level, per-vulnerability overview of vulnerabilities detected by Defender for Endpoint in the customers' environments. It allows you to search, sort, and filter the list of vulnerabilities. In addition, you can view a vulnerability's details such as exposed devices and affected software.

1. At MSP-level, navigate to [Reports > Vulnerabilities](#).

VULNERABILITIES						
				Search...	×	▼ Filter ⁰ As of Sep 12, 2024 12:49:48 PM
NAME ↕	ACCOUNTS AFFECTED ↕	ENDPOINTS AFFECTED ↕	CVSS/SEVERITY ↕	AGE (PUBLISHED/UPDATED) ↕	EXPLOIT TYPE ↕	
CVE-2023-52168	1	1	9.8 (Critical)	2 months (Jul 2, 2024 07:00 PM / Jul 31, 2024)	Remote	Properties
CVE-2024-30080	1	2	9.8 (Critical)	3 months (Jun 10, 2024 07:00 PM / Jun 13, 2024)	Remote	Properties
CVE-2024-38063	2	57	9.8 (Critical)	30 days (Aug 13, 2024 10:00 AM / Sep 10, 2024)	Remote	Properties
CVE-2024-38140	2	29	9.8 (Critical)	1 months (Aug 12, 2024 03:00 AM / Aug 16, 2024)	Remote	Properties
CVE-2024-38199	2	29	9.8 (Critical)	1 months (Aug 12, 2024 03:00 AM / Aug 15, 2024)	Remote	Properties
CVE-2022-28755	1	13	9.6 (Critical)	2 years (Aug 9, 2022 03:00 AM / Oct 24, 2022)	Not available	Properties
CVE-2023-39213	1	13	9.6 (Critical)	1 years (Aug 8, 2023 03:00 AM / Aug 15, 2023)	PrivilegeEscalation, Remote	Properties
CVE-2023-39216	1	5	9.6 (Critical)	1 years (Aug 8, 2023 03:00 AM / Aug 11, 2023)	PrivilegeEscalation, Remote	Properties

For any vulnerability, select [Properties](#) to see its details.

Day 1 – Lab 9 | Walkthrough

Vulnerability Dashboard



1. The [details](#) tab shows the details of the vulnerability.

VULNERABILITY CVE-2024-21417 DETAILS

Details

Exposed Devices

Affected Software

Description

Summary: A vulnerability has been discovered in the Text Services Framework component of Microsoft Windows, which could allow a local authenticated attacker to gain elevated privileges on the system. By executing a specially crafted program, the attacker could exploit this vulnerability to execute arbitrary code with higher privileges. Impact: If successfully exploited, this vulnerability could allow an authenticated attacker to execute arbitrary code with elevated privileges on the affected system. Remediation: Apply the latest patches and updates provided by the respective vendors. [Generated by AI]

Exploit Source URL

-

CVSS Vector

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

Exploit Verified

No

Exploit Kits

No

Exploit Type

PrivilegeEscalation

Close

2. The [Exposed devices](#) tab shows the devices that are exposed to the vulnerability.

VULNERABILITY CVE-2024-21417 DETAILS

Details

Exposed Devices

Affected Software

DEVICE NAME	ACCOUNT NAME	OS PLATFORM	ACTIONS
cpc-bhagy-v397y	Nube Hart, Inc.	Windows10	Open Device Page
admindesktop	Nube Hart, Inc.	Windows10	Open Device Page
test2p-cc2	Nube Hart, Inc.	Windows10WVD	Open Device Page
testaccp1-5-4	Nube Hart, Inc.	Windows10WVD	Open Device Page
s2	Nube Hart, Inc.	Windows10WVD	Open Device Page
cpc-bhagy-w1p6v	Nube Hart, Inc.	Windows10	Open Device Page
test-9aug1cc1	Nube Hart, Inc.	Windows10WVD	Open Device Page
test-10sep-cc	Nube Hart, Inc.	Windows10WVD	Open Device Page
mk	Nube Hart, Inc.	Windows10WVD	Open Device Page
rphpdigics-217d	Ganar Hart, Inc.	Windows10WVD	Open Device Page
test-cc-int1	Ganar Hart, Inc.	Windows10WVD	Open Device Page
rphpdigics-d94c	Ganar Hart, Inc.	Windows10WVD	Open Device Page
testp1-5-4	Ganar Hart, Inc.	Windows10WVD	Open Device Page

3. The [Affected Software](#) tab shows the software affected by the vulnerability.

VULNERABILITY CVE-2024-21417 DETAILS

Details

Exposed Devices

Affected Software

SOFTWARE	VULNERABLE VERSIONS
windows_10	10.0.19044, 10.0.19045
windows_11	10.0.22621

Day 1 - Lab 10

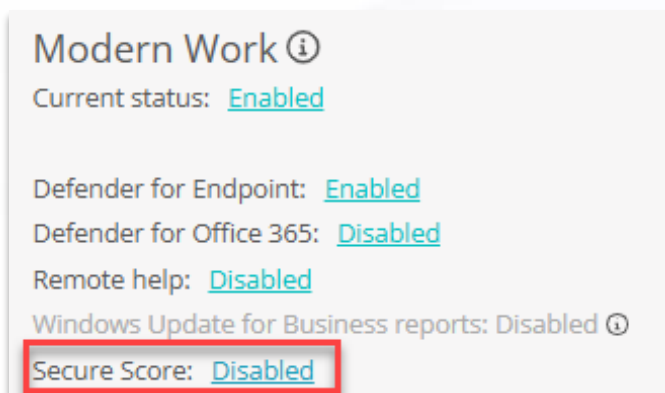


Day 1 – Lab 10 | Walkthrough




Secure Score



1. At the account level, navigate to [Settings > Integration](#).
2. In the [Modern Work](#) tile, next to [Secure Score](#), select [Disabled](#).



3. When prompted, confirm that you want to enable. At the account level, Secure Score is now included in the [Secure Scores](#) list.
4. At the account level, navigate to [Reports > Secure Score](#).

SECURE SCORE						
Secure Score-MSP						
Created by: k [redacted] m						
SECURE SCORE OVERVIEW ⓘ						  
ACCOUNT ⚙	TOTAL POINTS ACHIEVED ⚙	IDENTITY	DATA	DEVICE	APPS	
(1) Nube Hart, Inc.	65.22% (75/115)	85.19% (23/27)	100% (5/5)	none	56.63% (47/83)	View details
(7) Ganar Hart, Inc.	46.69% (484.67/1038)	40.91% (27/66)	0% (0/9)	50.02% (375.67/751)	38.68% (82/212)	View details
(91) Nerdio Golf Inc.	30.36% (17/56)	30.36% (17/56)	none	none	none	View details
3 items						

Note: Optionally, at the MSP level, you can create a Global View for Secure Scores. This is in addition to the navigation shown below.

Day 1 - Lab 11



Note: This section can only be completed on a Windows device.

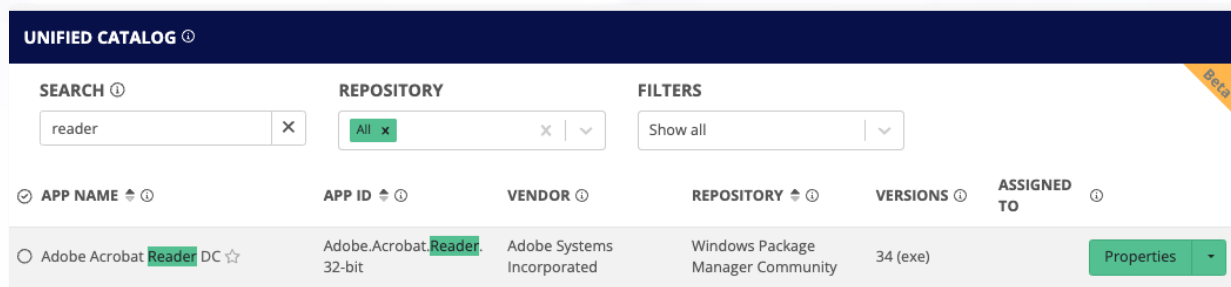
1. Open a PowerShell terminal in administrator mode.
2. Run the command `Winget --info`
 - *Returns a list of relevant locations, install folders, etc.*
3. Run the command `Winget Source List`
 - *Returns a list of Windows Package Manager sources.*
4. Run the command `Winget list`
 - *Returns a list of installed applications that can be managed via WinGet..*
5. Run the command `Winget upgrade`
 - *Returns a list of installed applications that have an available update.*
6. (Optional) Run the command `Winget upgrade --all`
 - *Updates all listed applications to the current version.*

Day 1 - Lab 11.1 | Walkthrough



Assigning Applications for UAM

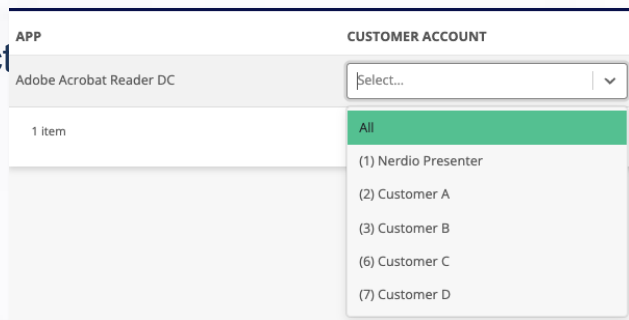
1. Expand the [Applications](#) blade and [search for the application](#) (MSP / Global level).



2. Click the [dropdown arrow](#) next to the app and select [Assign](#).



3. Use the [dropdown menu](#) to select accounts.



4. Click [Add Assignments](#) or [Apply and Close](#) to finish.

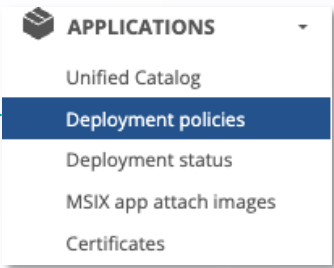


Day 1 - Lab 11.2 |

Create an application deployment policy



1. Expand the [Applications](#) blade and click [Deployment Policies](#) (customer account level).



2. Click [Add](#) to create a new policy.



3. In the *General* tab, give the policy a unique name, and click [Next](#).
(Leave the description blank)

NAME:

FCorpAppPolicy

DESCRIPTION:

4. In the *Applications* tab, select the apps to deploy and click [Next](#).
Type to search to find and select the following:

- *Adobe Acrobat Reader DC [latest]*
- *Mozilla Firefox [latest] (Public WinGet Community)*

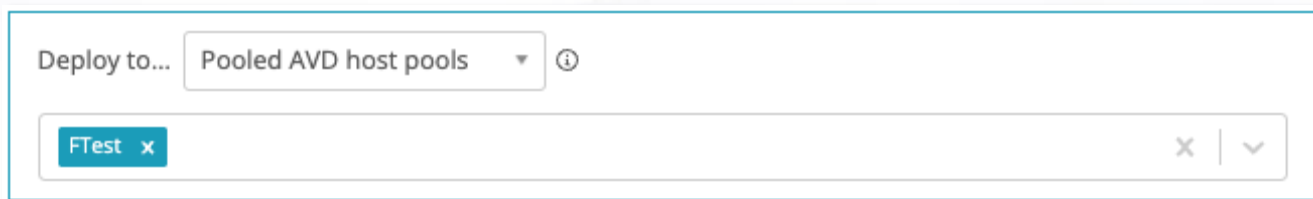
	NAME	INSTALL/UNINSTALL	ACTION NEEDED
≡	Adobe Acrobat Reader DC [latest] (Public MSStore)	<input checked="" type="radio"/> Install <input type="radio"/> Uninstall	<input type="checkbox"/> Reboot after install
≡	Mozilla Firefox [latest] (Public WinGet Community)	<input checked="" type="radio"/> Install <input type="radio"/> Uninstall	<input type="checkbox"/> Reboot after install
	Select applications ...		

Day 1 - Lab 11.2 |

Create an application deployment policy

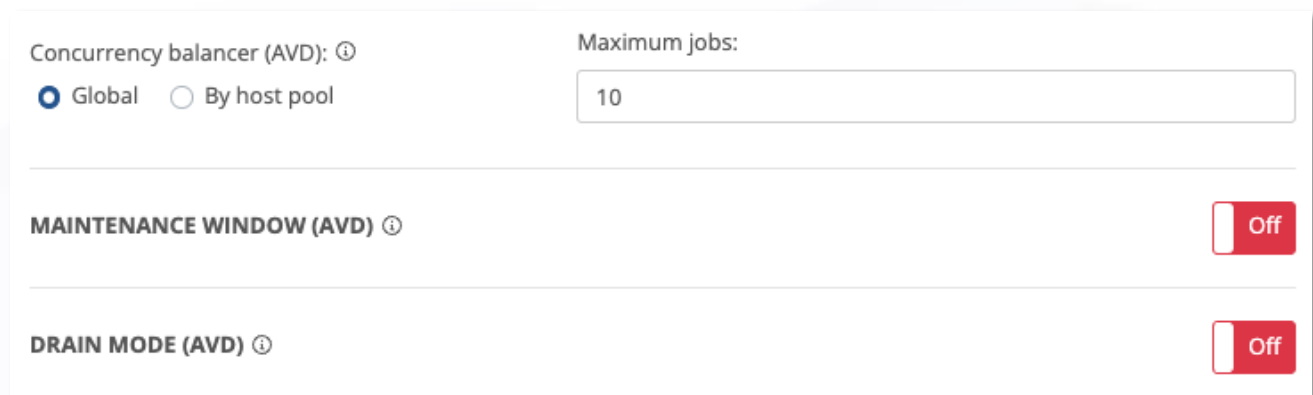
4. In the *Targets* tab, define where to apply the policy and click [Next](#).

- Toggle 'Deploy to...' to **Pooled AVD Host Pools**.
- Find and select the **host pool you created earlier**.



5. In the *Settings* tab, configure how tasks should execute.

- Set the 'Concurrency balancer' to **By Host Pool**.
- Change the 'Maximum Jobs' to **2**.



6. Click [Save & Close](#) to finish.



LAB GUIDE

MSP Foundations - Day 2



Day 2 - Lab 1

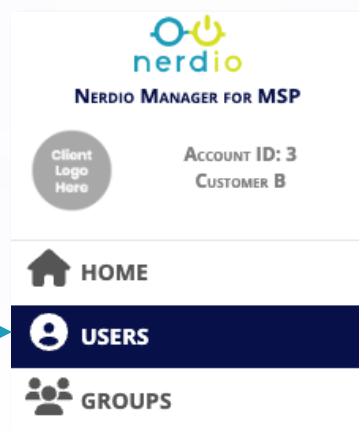


Day 2 - Lab 1 |

Add a Customer-Level User in NMM

1. Log into the customer account in NMM*.

1. See your email for a link to your assigned account.
2. If you don't have the email, send your business email in the chat to be added.



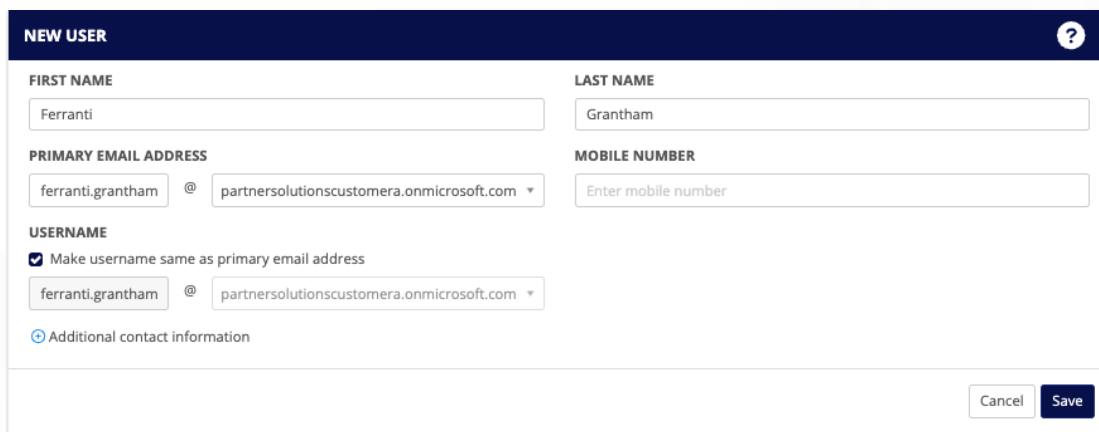
2. Click the [Users](#) blade.

3. Click [Add User](#).



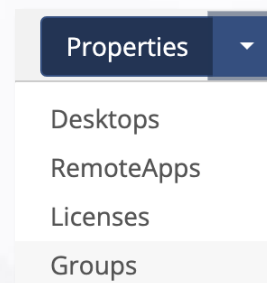
4. Enter the following user details:

- Your first name.
- Your last name.
- Set the primary email address to *Firstname.Lastname*.



5. Click [Save](#) and [OK](#) to dismiss the password prompt

6. Click the [dropdown](#) next to [Properties](#) for your user and select [Groups](#).



7. Select [MSP Training Camp Tech Day](#) from the list and click [OK](#) to add your user to the group.

Day 2 - Lab 2



How does the Approvals Workflow work?

All available tasks in Nerdio Manager are categorized as follows:

- **Destructive:** Delete a VM, delete a user, delete a host, delete a desktop image, delete a host pool, stop a global image, remove a global image, delete a NAT gateway, delete a group, delete a scripted action, etc.
- **Cost Impacting:** Change a VM's size, add a new disk to a server, activate/deactivate a host, power off a host, create a host pool, add a desktop image from a gallery, resize a desktop image, clone a desktop image, clone a host pool, start a global image, clone a global image, create a group, create a scripted action, link/unlink a resource group, etc.
- **User Impacting:** Restart a VM, log off a user, power off and set as image, log off users, send a message to a host, run a scripted action, etc.
- **Setting Changes:** Update host pool properties, update AD settings, update FSLogix settings, add/update Global FSLogix settings, update host properties, create an NSG, create peering, edit a VPN connection, edit NSG rules, etc.

In addition to the built-in task categories noted above, Nerdio Manager allows MSPs to create custom task categories.

Nerdio Manager allows MSPs to configure approval rules for selected tasks and user roles.

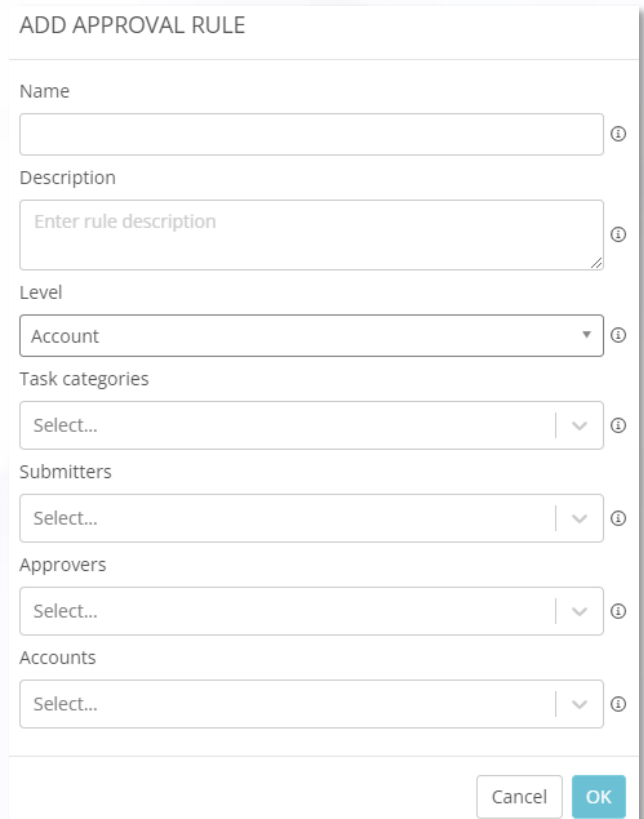
Manage Task Categories

Nerdio Manager allows you to manage task categories. This includes creating, changing, copying, and removing custom task categories. In addition, you can create a copy of a built-in task category.

Manage Approval Rules

Nerdio Manager allows you to manage approval rules. This includes creating, changing, copying, and removing approval rules.

1. Navigate to [Workflows > Approval Rules](#).
2. Select [ADD](#).
3. Fill out the details.
4. Click [OK](#).



The screenshot shows the 'ADD APPROVAL RULE' form. It contains the following fields and controls:

- Name:** A text input field with an information icon.
- Description:** A text input field with the placeholder 'Enter rule description' and an information icon.
- Level:** A dropdown menu currently showing 'Account' with an information icon.
- Task categories:** A dropdown menu with 'Select...' and a downward arrow, with an information icon.
- Submitters:** A dropdown menu with 'Select...' and a downward arrow, with an information icon.
- Approvers:** A dropdown menu with 'Select...' and a downward arrow, with an information icon.
- Accounts:** A dropdown menu with 'Select...' and a downward arrow, with an information icon.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

Task Categories:

- Choose a pre-canned/custom
- Choose different categories

Approval Rules:

- Use pre-canned or custom
- MSP or customer level
- Assign staff to **submitters** and **approvers** groups.

Notification Conditions

Nerdio Manager allows you to specify which actions or states trigger a notification. You can create conditions for tasks, reservations, usage, backup, Intune, and Defender.

Create a new condition

1. Navigate to [Notifications](#) at the MSP level.
2. Select [ADD](#).
3. Fill out the details.
4. Click [OK](#).

NOTIFICATIONS - CREATE CONDITION

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

NAME:	<input type="text"/>	?
NOTIFICATION TYPE:	Task condition	?
ACCOUNTS:	<div>Any ×</div>	× ▼ ?
TARGETS:	<div>Any ×</div>	× ▼ ?
TASKS:	<div>Any ×</div>	× ▼ ?
RUN BY :	<div>Any ×</div>	× ▼ ?
STATUSES:	<div>Any ×</div>	× ▼ ?

Cancel OK

Notes:

- You can set up conditions for tasks, behaviors and statuses.
- These can be applied to individual accounts, all accounts or a group of accounts.
- Conditions can also be focused to specific users.

Notification Actions

Actions are the notifications to send out if a condition is matched. You may send out a notification via email or custom API.

Create a new action

1. Navigate to [Notifications > Actions](#) at the MSP level.
2. Select [ADD](#).
3. Fill out the details.
4. Click [OK](#).

NOTIFICATIONS - CREATE ACTION

Specify how you would like to get notified. When you choose to get notified by email, please specify the source and destination addresses. If you choose to get notified by a POST to a custom API endpoint, make sure your API is within reach to you NMM install.

CONDITIONS: *

Select... | v ⓘ

☒ EMAIL NOTIFICATION

SEND FROM:

Select... | v ⓘ

SEND TO: *

 ⓘ

☐ Include task detail ⓘ

☒ CUSTOM API NOTIFICATION

CUSTOM API ENDPOINT: *

Enter URL ⓘ

CUSTOM API KEY:

Enter API key ⓘ

[Show request sample v](#)

Cancel

OK

Notes:

- *Creating actions will let you define notification behaviors by selecting destination emails and condition(s) to trigger a notification event.*
- *You can link your own account or choose an automatically created email from the portal.*
- *You can also choose to be notified via Rest API (API must be within reach of the NMM install).*

Day 2 - Lab 3



What is FSLogix?

1. A user profile container technology.
2. Allows user profiles to roam without losing their customizations.

How does it work?

1. Requires a storage service for profile containers.
 - *(E.g., Azure Files)*
2. Installation of the FSLogix application.
 - *Nerdio automatically installs by default when a new session host is created.*
3. Create FSLogix configuration profiles in Nerdio.
 - *Assign these profiles to customer accounts for centralized management.*

Azure Files

1. Microsoft recommends Premium storage in Azure Files.
2. Lower tiers of storage may cause errors in daily operations.
3. Premium Storage for Azure Files is Nerdio auto-scale compatible.
 - Nerdio auto-scaling ensures there is always enough storage available.

Storage Options

1. UNC Path (File Server)
2. Azure Files (Premium)

[See this Nerdio Help Center article for more information on configuring FSLogix.](#)

What is an RDP Profile?

1. A configuration created in Nerdio that defines the RDP experience for users.

How do RDP Profiles work?

1. Can be created at the global level and then cascaded to customer accounts.
 - *RDP profiles can also be created at the customer account level for granular customization.*
2. Once created, RDP Profiles are assigned to host pools, which are then inherited by all hosts within the pool.

Key items to configure

audiocapturemode

- *Defines whether audio input can be redirected from the local device to the session.*

camerastoredirect

- *Makes the local webcam / camera available in the session.*

devicestoredirect

- *Allows plug in devices to appear in the session(E.g., flash drives).*

drivestoredirect

- *Redirects drives from the local machine to the session.*

redirectprinters

- *Allows local printers to be made available in the session.*

redirectclipboard

- *Allows clipboard sharing between the local device and session.*

Remember, always consider compliance requirements!

[See this Nerdio Help Center article for more information on configuring Global RDP Profiles.](#)

Day 2 - Lab 4



Day 2 - Lab 4 |

Create an Image Source VM



1. Click the [Desktop Images](#) blade (customer account level).



2. Click [Add from Azure Library](#).



3. Add the following parameters to your image source VM.

Name	Enter a unique name. Save the name for later!
Description	Leave this blank
Azure Image	Windows 11 (22H2) Enterprise multi-session + Microsoft 365 Apps – Gen2 (multi-session)
VM Size	D2s_v5 (2C & 8GB @ \$0.19/hr retail)
OS Disk	E10 (128 GB Premium SSD @ \$0.03/hr retail)
Trusted Launch	Check the box to enable. (Required for Gen2 VMs)
Join to AD – FSLogix App	Leave these settings at default.
Local admin credentials	Create unique credentials (do not use “admin”). Save these for use later!
Turn on Geographic distribution & Azure Compute Gallery	Select NMMACDSUB#. Leave the region set to East US. Leave the storage at default.
Click OK to create the image source VM.	

ADD DESKTOP IMAGE ⓘ

Add desktop image from Azure image library.

NAME:	<input type="text" value="FerrantiCorpIMG"/>	ⓘ
DESCRIPTION:	<input type="text"/>	ⓘ
AZURE IMAGE:	<input type="text" value="Windows 11 Enterprise multi-session + Microsoft 365 Apps - Gen2 (..."/>	ⓘ
VM SIZE:	<input type="text" value="D4s_v5 (4C & 16GB @ \$0.19/hr retail)"/>	ⓘ
OS DISK:	<input type="text" value="D2s_v5 (2C & 8GB @ \$0.10/hr retail)"/> <input type="text" value="E10 (128 GB Standard SSD @ \$0.01/hr retail)"/>	ⓘ

☒ Use Trusted Launch ⓘ

☐ Join to AD ⓘ

☐ Do not create image object ⓘ

☒ Enable time zone redirection ⓘ

☒ Set time zone:

☐ Install certificates ⓘ

☒ Uninstall FSLogix app ⓘ

Provide custom credentials for a local administrator user

On

USERNAME:

PASSWORD:

Geographic distribution & Azure compute gallery

On

AZURE COMPUTE GALLERY:

AZURE REGIONS:

STORAGE ACCOUNT TYPE:

Run the following scripted actions:

Off

Applications Management BETA

Off

This task may take up to a few hours to complete. You can monitor progress in the Desktop Images Tasks section.

Cancel

OK

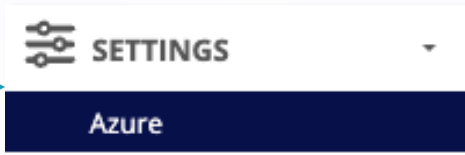
Day 2 - Lab 5



Day 2 - Lab 5.1 | Walkthrough

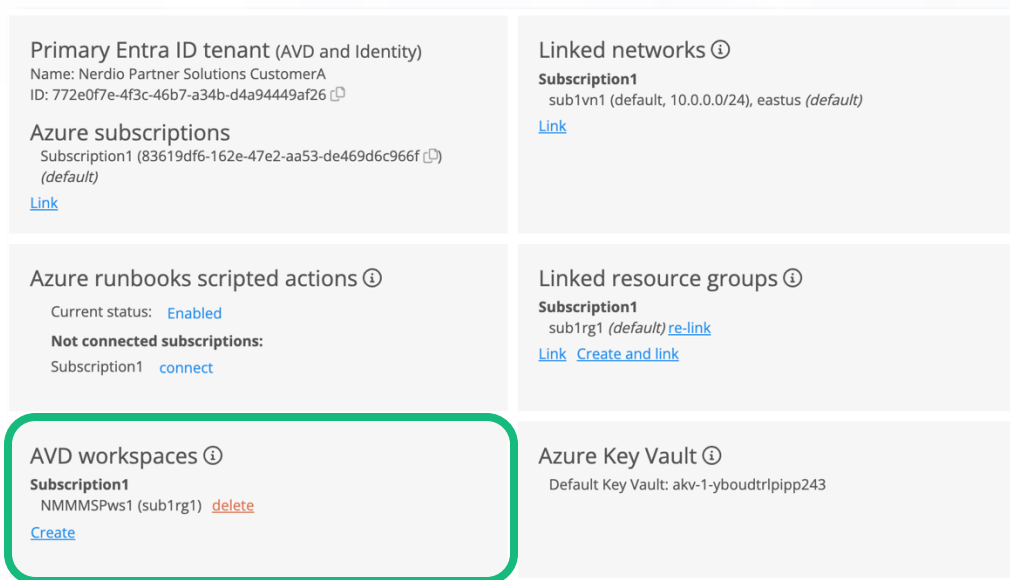
Add AVD Workspaces in NMM

1. Expand the [Settings](#) blade and click [Azure \(customer account level\)](#)

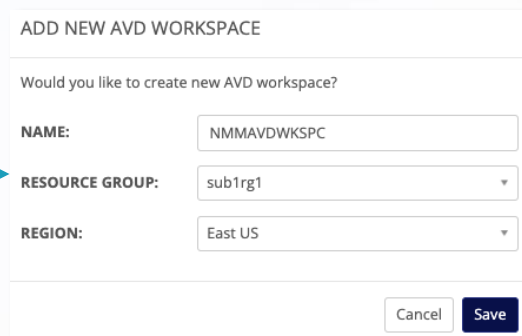


2. Click [Create](#) in the [AVD Workspaces list](#).

- Existing workspaces in the Resource Group will appear here automatically.



3. Enter a name and select a resource group and region.

A screenshot of the 'ADD NEW AVD WORKSPACE' form. It asks 'Would you like to create new AVD workspace?' and has three input fields: 'NAME' (filled with 'NMMAVDWKSPC'), 'RESOURCE GROUP' (filled with 'sub1rg1'), and 'REGION' (filled with 'East US'). There are 'Cancel' and 'Save' buttons at the bottom right.

4. Click [Save](#) to finish.

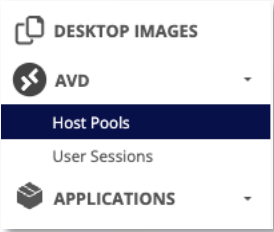


Day 2 - Lab 5.2 |

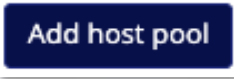
Create a host pool



1. Expand the [AVD blade](#) and click [Host Pools \(customer account level\)](#).



2. Click [Add Host Pool](#).



3. Add the following parameters to your host pool.

Name	Enter a unique name (this is what appears on the user's desktop. (Save the name for later!))
Description	Leave this blank
Desktop / App Experience	Multi-User Desktop
Directory	Leave at default.
FSLogix	Leave at default.
Name Prefix	Choose a unique name for your hosts. Each host will be appended with "-xxxx".
Desktop Image	Windows 10 (22H2) EVD + MS 365 Apps - Gen2 (multi-session)
VM Size	D2s_v5 (2C & 8GB @ \$0.10/hr retail)
OS Disk	E10 (128 GB Standard SSD @ \$0.01/hr retail)
Quick Assign	Type MSP Training Camp Tech Day and select it.
Trusted Launch	Leave this box checked to enable Trusted Launch.

Click **OK** to create your host pool.

ADD HOST POOL ⓘ

NAME:

FerrantiCorpHP ⓘ

DESCRIPTION:

Enter description for admin users ⓘ

DESKTOP/APP EXPERIENCE: ⓘ

- ☒ Multi user desktop (pooled) ⓘ
- ☐ Multi user RemoteApp (pooled) ⓘ
- ☐ Single user desktop (pooled) ⓘ
- ☐ Single user desktop (personal) ⓘ

DIRECTORY:

Default (Entra ID) ⓘ

FSLOGIX:

OFF ⓘ

There are several limitations, including limited support for FSLogix. Review Microsoft's [MFA requirements](#) for Microsoft Entra joined VMs. [Learn more](#)

NAME PREFIX:

FCorpHost

Prefix ⓘ

DESKTOP IMAGE:

Windows 10 (22H2) EVD + MS 365 Apps - Gen2 (multi-session) ⓘ

VM SIZE:

D2s_v5 (2C & 8GB @ \$0.10/hr retail) ⓘ

OS DISK:

E10 (128 GB Standard SSD @ \$0.01/hr retail) ⓘ

QUICK ASSIGN:

 MSP Training Camp Tech Day (MSPTrainingCampTechI x ⓘ

☒ Use Trusted Launch ⓘ

This task may take a long time to complete. You can monitor progress in the Host Pools Tasks section.

Cancel

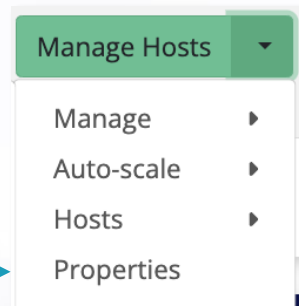
OK

Day 2 - Lab 5.3 |

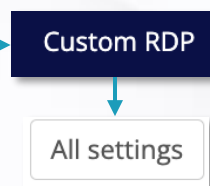
Adjust Host Pool Settings

1. Find your host pool in [AVD > Host Pools](#) (customer account level).

2. Click the dropdown arrow next to [Manage Hosts](#) and select [Properties](#).



4. Click the [Custom RDP](#) tab.



5. Click [All Settings](#).

6. Use the dropdown to toggle to the [MSP Foundations Training Camp RDP Config](#).



7. Check the box to [Sync RDP settings with Global Properties](#).



- This setting allows changes made at the Global / MSP level to be applied here.

8. Scroll to the bottom and click [Save](#) to assign the profile settings.

Day 2 - Lab 5.4 |

Deploy Session Hosts



1. Click [Manage Hosts](#) next to your host pool in the [AVD blade > Host Pools](#) (customer account level).



2. Click [Add Session Host](#).



3. Add the following parameters to create two session hosts.

Host Count	Set to 2 .
Name Prefix	Use the same prefix as the host pool.
Append a Suffix	Leave checked.
Desktop Image	Windows 10 (22H2) EVD + MS 365 Apps - Gen2 (multi-session)
VM Size	D2s_v5 (2C & 8GB @ \$0.10/hr retail)
OS Disk	E10 (128 GB Standard SSD @ \$0.02/hr retail)
Custom OS Disk Size (GiB)	Leave at default (128).
Do Not Activate	Leave unchecked.
Process hosts in groups of:	Set to 2 .
Number of failures before aborting:	Leave at 5 .

Click **OK** to create your session hosts.

ADD HOST TO POOL ⓘ

If Autoscaling is enabled the newly added host may be deleted or stopped to comply with dynamic auto-scaling parameters.

HOST POOL: FerrantiCorpHP

DESKTOP/APP EXPERIENCE: Multi user desktop (pooled)

HOST COUNT: ⓘ

HOST NAME: Prefix ⓘ

DESKTOP IMAGE: Windows 10 (22H2) EVD + MS 365 Apps - Gen2 (multi-... ⓘ

VM SIZE: D2s_v5 (2C & 8GB @ \$0.10/hr retail) ⓘ

OS DISK: E10 (128 GB Standard SSD @ \$0.01/hr retail) ⓘ

CUSTOM OS DISK SIZE (GIB): ⓘ

DO NOT ACTIVATE: ☐ ⓘ

Process hosts in groups of: ⓘ

Number of failures before aborting: ⓘ

With the schedule set to OFF action will be performed immediately. With schedule turned ON, the task will be performed according to the specified schedule.

SCHEDULE

☐ Off ⓘ

Cancel

OK

Day 2 - Lab 6



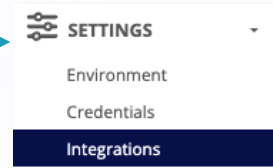
Day 2 - Lab 6.1 | Walkthrough

Scripted Actions



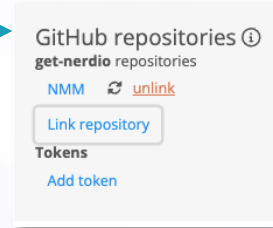
Connect a GitHub Repository

1. Open the [Setting blade](#) and click [Integrations](#) (MSP / Global level).



2. Click [Link Repository](#) and supply:

- GitHub account name
- GitHub repository name
- GitHub access token



GitHub Account ⓘ

GitHub Repository ⓘ

GitHub access token ⓘ

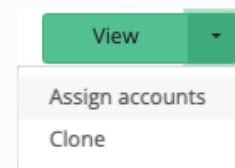
3. Click [OK](#) to link.

Assign Scripted Actions to Customer Accounts

1. Open the [Scripted Actions blade](#) and click [Windows Scripts](#) or [Azure Runbooks](#) (MSP / Global level).



2. Find the target script(s) and click the [dropdown arrow > Assign accounts](#).



3. Select accounts using the [dropdown menu](#), then click [OK](#) when finished.

ASSIGN ACCOUNTS TO INSTALL EGNYTE SCRIPTED ACTION

Do you want to assign selected accounts to Install Egnyte?
Note: Accounts removed from that list will lose access to this scripted action.

Select...

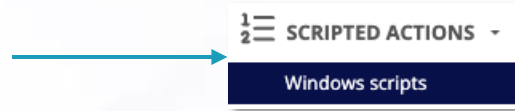
Day 2 - Lab 5.1 | Walkthrough

Scripted Actions



Add new Scripted Actions

1. Open the [Scripted Actions blade](#) and click [Windows Scripts](#) or [Azure Runbooks](#) (MSP / Global level).



2. Click [Add Scripted Action](#).



3. Provide the following:

- A name for the Scripted Action
- A description (if applicable)
- Tag(s)
- A script execution mode
 - *E.g., Individual, Individual with restart, combined*

CREATE SCRIPTED ACTION

Create a new scripted action that can be re-used throughout Nerdio Manager for MSP

NAME:

DESCRIPTION:

TAGS:

SCRIPT EXECUTION MODE:

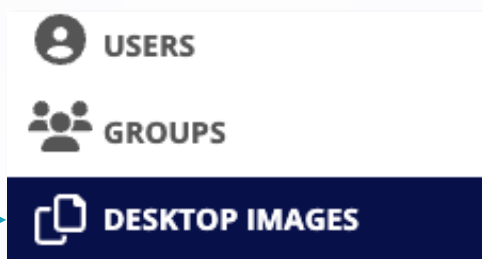
Hide

4. Expand the [Show](#) menu and enter script. Click [OK](#) when finished.

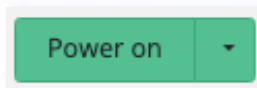
Day 2 - Lab 6.2 |

Update the Image Source VM

1. Click the [Desktop Images](#) blade (customer account level).



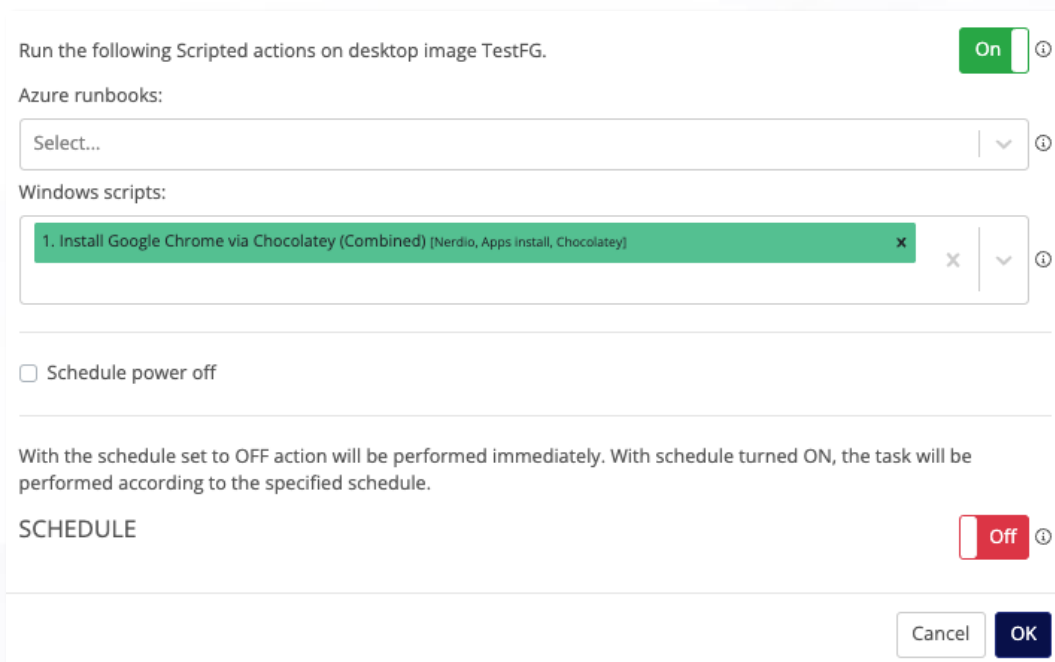
2. Find your image and click [Power On](#).



3. Turn [Run the following scripted actions](#) to [On](#).

4. Select [Install Google Chrome](#) from the [Windows Script](#) list.

- *For time, we'll use these scripts as a demonstration.*
- *In practice, use scripted actions to automate updates.*



5. Do not schedule power off. Click [cancel](#).

We'll run this script in a later lab.

Day 2 - Lab 6.3 |

Create an image



1. Find the image source VM you created.
2. Click [Power off & set as image](#) or [Set as image](#).
3. Turn [Run the following scripted actions before set as image](#) to [ON](#).
4. Select [Install Google Chrome via Chocolatey](#) under [Windows Scripts](#).
5. Change the [Target](#) to [Source](#).
6. Leave other settings at their default and click [OK](#).

Day 2 - Lab 6.3 |

Create an image

Geographic distribution & Azure compute gallery ⓘ

AZURE COMPUTE GALLERY: NMMACDSub1 x ⓘ

AZURE REGIONS: East US x ⓘ

STORAGE ACCOUNT TYPE: Standard HDD ⓘ

☐ Stage new image as inactive ⓘ

Run the following scripted actions before set as image: On ⓘ

Azure runbooks: Select... ⓘ

Windows scripts:

1. Install Google Chrome via Chocolatey (Combined) [Nerdio, Apps install, Chocolatey] x ⓘ

Target VM: ⓘ ☐ Clone ☒ Source

Applications Management Off ⓘ

Error Handling Off ⓘ

☒ Retain current image object ⓘ Versions to keep: 3 ⓘ

☐ Install certificates ⓘ

☐ Validate image ⓘ

Change log: ⓘ

There are known issues with Sysprep in Windows 11 22H2. Please apply the scripted action [Windows 11 22H2 - Modify Sysprep] to resolve.

Day 2 - Lab 7



Day 2 - Lab 7 |

Re-image session hosts

1. Expand the action menu next to your host pool in [AVD > Host Pools](#).

Manage Hosts

2. Then click [Resize / Re-image](#) under the [Hosts](#) tree.

Add new

Resize/Re-image

Restart

3. Toggle the [Desktop Image](#) to the custom image you created earlier.

4. Turn off [Messaging](#) and click [OK](#).

5. Click [OK](#).

RESIZE OR RE-IMAGE HOSTS ⓘ

▶ Run now📅

Resize or re-image hosts in MSP TC Sales Chicago. You can change the desktop image, VM size and/or OS disk. Changes will apply to all session hosts. The selected parameters will also be set as the default for future hosts that are added.

DESKTOP IMAGE:

DeathStar (Jul 8, 2024/2.0.0) ⓘ

VM SIZE:

No change ⓘ

OS DISK:

No change ⓘ

CUSTOM OS DISK SIZE (GIB):

ⓘ

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

MESSAGING

Off ⓘ

Process hosts in groups of:

2 ⓘ

Number of failures before aborting:

5 ⓘ

CancelOK

Day 2 - Lab 8

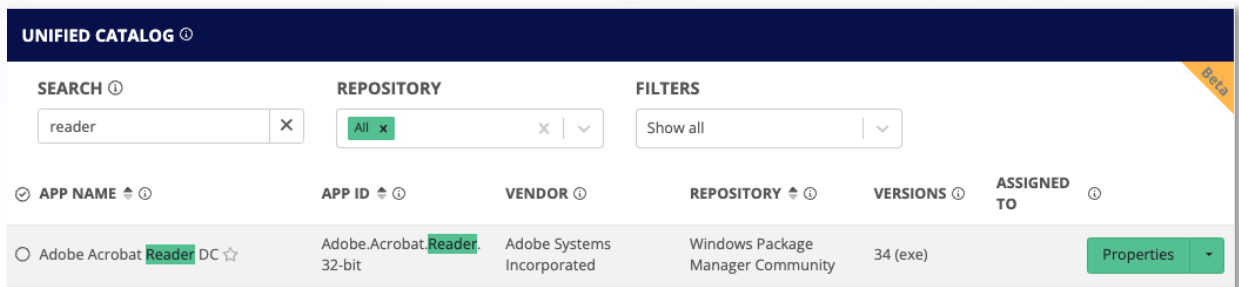


Day 2 - Lab 8.1 | Walkthrough

Assigning Applications for UAM



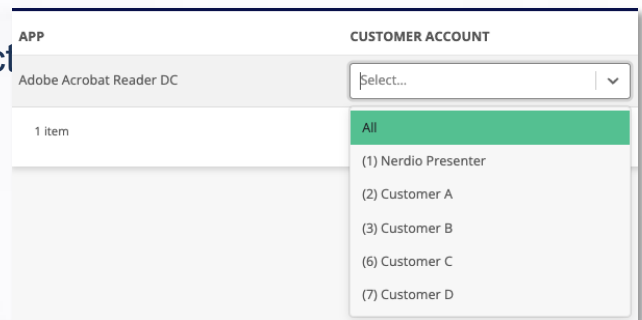
1. Expand the [Applications](#) blade and [search for the application](#) (MSP / Global level).



2. Click the [dropdown arrow](#) next to the app and select [Assign](#).



3. Use the [dropdown menu](#) to select accounts.



4. Click [Add Assignments](#) or [Apply and Close](#) to finish.

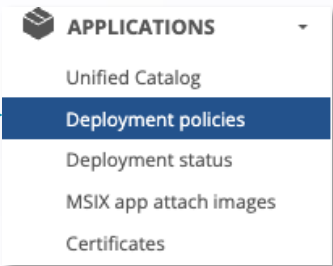


Day 2 - Lab 8.2 |

Create an application deployment policy



1. Expand the [Applications](#) blade and click [Deployment Policies](#) (customer account level).



2. Click [Add](#) to create a new policy.



3. In the *General* tab, give the policy a unique name, and click [Next](#).
(Leave the description blank)

NAME:

FCorpAppPolicy

DESCRIPTION:

4. In the *Applications* tab, select the apps to deploy and click [Next](#).
Type to search to find and select the following:

- *Adobe Acrobat Reader DC [latest]*
- *Mozilla Firefox [latest] (Public WinGet Community)*

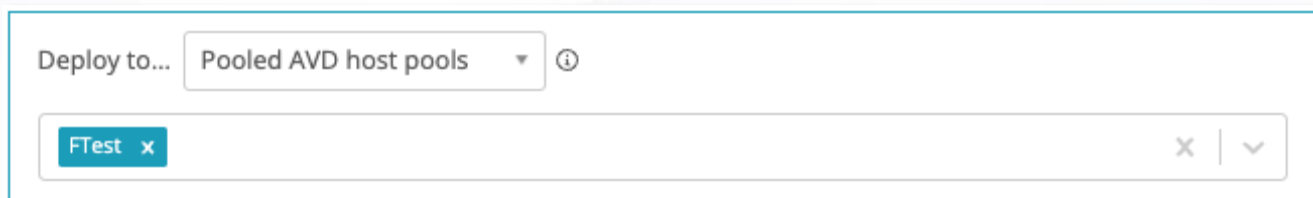
	NAME	INSTALL/UNINSTALL	ACTION NEEDED
≡	Adobe Acrobat Reader DC [latest] (Public MSStore)	<input checked="" type="radio"/> Install <input type="radio"/> Uninstall	<input type="checkbox"/> Reboot after install
≡	Mozilla Firefox [latest] (Public WinGet Community)	<input checked="" type="radio"/> Install <input type="radio"/> Uninstall	<input type="checkbox"/> Reboot after install
	Select applications ...		

Day 2 - Lab 8.2 |

Create an application deployment policy

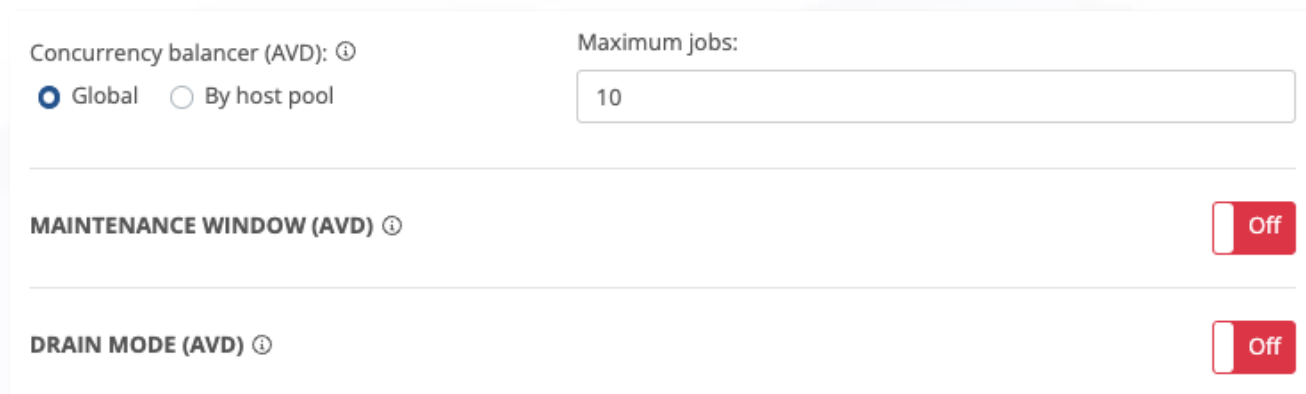
4. In the *Targets* tab, define where to apply the policy and click [Next](#).

- Toggle 'Deploy to...' to **Pooled AVD Host Pools**.
- Find and select the **host pool you created earlier**.



5. In the *Settings* tab, configure how tasks should execute.

- Set the 'Concurrency balancer' to **By Host Pool**.
- Change the 'Maximum Jobs' to **2**.



6. Click [Save & Close](#) to finish.

Save & close

Day 2 - Lab 9



1. Navigate to [Customer > Azure Files](#)

 AZURE FILES

2. Then click the down arrow next to [Manage](#) for the share you want to work with.

Manage

▼

3. Select [Configure](#) in the menu.

Configure

History

Force start

Auto-scale ▶

File handles

Copy UNC path

Unlink

4. Configure the [Provisioned Size \(quota\)](#) section. Default settings can work to scale OUT when it gets within 10%.

1

PROVISIONED SIZE (QUOTA) ⓘ

Quota unit:

Relative (%) ⓘ

Minimum size: used capacity (0.32 GiB) +

10

 % (100 GiB) ⓘ

Maximum size: used capacity (0.32 GiB) +

100

 %

less than

102400

 GiB (100 GiB) ⓘ

PERFORMANCE

	MINIMUM	MAXIMUM
BASELINE IO/S ⓘ	500	500
BURST IO/S ⓘ	4000	4000
EGRESS RATE ⓘ	66.00 MiBytes/s	66.00 MiBytes/s
INGRESS RATE ⓘ	44.00 MiBytes/s	44.00 MiBytes/s

5. Configure the [Scaling logic](#) section, if need be. This will scale OUT when the average or maximum time used to process a request by Azure storage is slower.

3

SCALING LOGIC ⓘ

Select auto-scale trigger:

Success Server Latency (avg) ⓘ

Increase quota (scale out) by

10

 % if Success Server Latency exceeds

20

 ms for

5

 minutes (current latency: 1.67 ms)

Decrease quota (scale in) by

20

 % if Success Server Latency drops below

10

 ms for

15

 minutes (current latency: 1.67 ms)

Provisioned size (quota) can be decreased only 24 hours after the last quota increase. Last quota increase: Nov 21, 2024 04:27 PM

Day 2 - Lab 9.2 | Walkthrough

Configure Auto-scale (Pooled)



1. Expand the action menu next to your host pool in [AVD > Host Pools](#).

Manage Hosts

2. Then click [Configure](#) next in the [Auto-scale](#) tree.

Configure

History

Force start

Pause autoscale

To keep API call volume low, please do not turn Auto-scale on in the lab sandbox environments.

3. Select the [Desktop Image](#) you created earlier.

Hosts will be provisioned based on the template for pool:

NAME PREFIX:

FTest

DESKTOP IMAGE (TEMPLATE):

TestFG (Nov 28, 2023/2.0.0)

VM SIZE (TEMPLATE):

D2s_v3 (2C & 8GB @ \$0.10/hr retail)

4. Configure each section to match the associated screenshot.

1 HOST POOL SIZING ⓘ

Active host defined as: AVD agent Available ⓘ

Base host pool capacity: 2 host(s) in the pool ⓘ

Min active host capacity: 1 host(s) in the pool ⓘ

Burst beyond base capacity: up to 1 extra host(s) in the pool ⓘ

2 SCALING LOGIC ⓘ

Pool settings

Session limit per host: 10 Maximum host pool sessions: 30

Load balancing: Depth First ⓘ

☐ Start on Connect

Triggers (scale out on **ANY** condition, scale in on **ALL** conditions) ⓘ

Select autoscale trigger: CPU usage ⓘ

Start or create (scale out) up to 1 host(s) if CPU utilization across all hosts exceeds 65 % for 5 minutes ⓘ

Stop or remove (scale in) up to 1 host(s) if CPU utilization across all hosts drops below 40 % for 15 minutes ⓘ

+ add trigger

Scale in restrictions

Stop or remove (scale in) hosts only from: 6 p.m. to: 5 a.m. ⓘ

Scale in aggressiveness: High ⓘ

Scale in burst host selection: Host with fe... ⓘ

Day 2 - Lab 9.2 | Walkthrough

Configure Auto-scale (Pooled)



3 ROLLING DRAIN MODE ⓘ

On

Window name ⓘ Start time ⓘ % hosts in drain mode ⓘ

[+ add window](#)

4 PRE-STAGE HOSTS ⓘ

On

☐ Use multiple schedules ⓘ

Work days: ⓘ

Start of work hours: ⓘ

Hosts to be active by start of work hours: ⓘ

Scale in delay: ⓘ

Notify if isn't done: ⓘ

5 MESSAGING ⓘ

Send a warning message to users on the host: before scaling in host

The message should say: ⓘ

Sorry for the interruption. We are doing some housekeeping and need you to log out. You can log in right away to continue working. We will be terminating your session in 10 minutes if you haven't logged out by then.

6 AUTO-HEAL BROKEN HOSTS ⓘ

On

Auto-scale can automatically attempt to repair "broken" session hosts by restarting them, running one or more scripted actions, and deleting/recreating them. It can make a few attempts to restart the host to try to get it back into operational state, then run scripted actions, and then either leave it alone or delete and re-create the host.

Host is broken if AVD agent status is: and ⓘ

Number of restart attempts: ⓘ

Minutes between restarts: ⓘ

Run Scripted actions after restart attempts: ⓘ

Unrecoverable hosts should be: ⓘ

5. When you are finished, click [Save](#).

Save

To keep API call volume low, please do not turn Auto-scale on in the lab sandbox environments.

Day 2 - Lab 9.3 | Walkthrough

Configure Auto-scale profiles (Schedule-based)



1. Navigate to [Settings](#) at the global/MSP level. Then click [Add auto-scale profile](#).



Auto-scale Profiles

2. Choose the Auto-scale mode: Schedule-based (Personal)

PROFILE SETTINGS

Auto-scale mode:

Name:

Description:

Default (Pooled) ▲

Default (Pooled)

Schedule-based (Personal)

User-driven (Personal)

3. Configure the global profile settings and click [Save](#).

1 HOST POOL PROPERTIES ⓘ

☐ Start on Connect

2 WORKING HOURS ⓘ

Monday - Friday ▼

8 a.m. ▼ to: 6 p.m. ▼

Power off aggressiveness: Medium ▼ ⓘ

Power on timing: Once ▼ ⓘ

Power off timing: Continuously ▼ ⓘ

3 MESSAGING ⓘ

Send a warning message to active users: 10 minutes ▼ before powering off the desktop.

The message should say: ⓘ

Sorry for the interruption. We are doing some housekeeping and need you to log out. You can log in right away to continue working. We will be terminating your session in 10 minutes if you haven't logged out by then.

Cancel

Save

Day 2 - Lab 9.3 | Walkthrough

Configure Auto-scale profiles



4. Next, you have to assign these profiles to the needed host pools.

Click the dropdown next to the profile and choose [Assignments](#).

5. Click on [Add Assignments](#) select the profile, host pools, and schedule. Then click [Confirm](#).

ADD HOST POOL AUTO-SCALE PROFILE ASSIGNMENTS

Auto-scale profile:

Select auto-scale profile



Host pools:

Select...



Schedule type:

Default schedule



Cancel

Confirm

1. Navigate to [Settings](#) at the global/MSP level. Then click [Add auto-scale profile](#).



2. Choose the Auto-scale mode: User-driven (Personal)

PROFILE SETTINGS

Auto-scale mode:

Name:

Description:

Default (Pooled)

Default (Pooled)

Schedule-based (Personal)

User-driven (Personal)

3. Configure the global profile settings and click [Save](#).

1 HOST POOL PROPERTIES ⓘ

☐ Start on Connect

2 DESKTOP START AND STOP

Desktops are started when users connect

Desktops are stopped when users log off after 10 minutes ⓘ

3 PRE-STAGE HOST OS DISKS ⓘ

Off

Cancel

Save

Day 2 - Lab 9.3 | Walkthrough

Configure Auto-scale profiles



4. Next, you have to assign these profiles to the needed host pools.

Click the dropdown next to the profile and choose [Assignments](#).

5. Click on [Add Assignments](#) select the profile, host pools, and schedule. Then click [Confirm](#).

ADD HOST POOL AUTO-SCALE PROFILE ASSIGNMENTS

Auto-scale profile:

Select auto-scale profile



Host pools:

Select...



Schedule type:

Default schedule



Cancel

Confirm

Day 2 - Lab 10



Day 2 - Lab 10.1 | Walkthrough



Create a new backup policy

Notes:

You must create one policy for Azure Files shares and a second for virtual machines (including servers, session hosts and image source VMs). Vaults typically have at least two policies.

1. Go to [Customer > Settings > Integrations](#).
2. In the [Backup recovery vaults, policies and assignments](#) tile, locate the vault you wish to work with.
3. Select [Add policy](#).
4. Enter the needed info.
5. Choose your retention settings for [daily](#), [weekly](#), [monthly](#), and [yearly](#).

ADD POLICY

Would you like to create a new Backup Policy?

NAME:

TYPE:

FREQUENCY:

RETENTION: ☒ Daily ☐ Weekly ☐ Monthly ☐ Yearly

☒ On **Retention of daily backup point**

Duration (days)

SNAPSHOT:

With the schedule set to OFF there will be no backups validation. With schedule turned ON, the backups validation will be performed according to the specified schedule.

BACKUP VALIDATION SCHEDULE ☒ On

Start date:

Time zone:

Start time: :

REPEAT:

☐ Use Boot Diagnostic Insights

☐ Disable Virtual Machine Internet Access during Validation

Day 2 - Lab 10.1 | Walkthrough



Assign a new backup policy

Notes:

Assignments determine what is to be protected. Assignment must be done by Azure region as determined by the region you selected for the vault when you first created it.

1. Go to [Customer > Settings > Integrations](#).
2. In the [Backup recovery vaults, policies and assignments](#) tile, scroll down to [Protection regions](#).
3. Locate the protected region you wish to work with, select [Assign policy to resources](#).
4. Select the backup policy for each of the resources.
5. Once you have entered all the desired info, select [Save](#).

Protected regions:

australia...	5 resources assigned	Assign policy to resources
northcen...	5 resources assigned	Assign policy to resources

SET RESOURCE BACKUP POLICY

Configure backup settings for **australiaeast** region

Desktop images

spdaily1511

Azure Files shares

sp151101

Servers

spdaily1511

Personal session hosts

spdaily1511

Pooled session hosts

spdaily1511

Cancel

Save

Day 2 - Lab 10.2 | Walkthrough



Enable backups for Azure resources

1. Go to [Customer > Backup](#). Then choose [Enable backup](#) on the resource you want to protect.

Enable backup

2. Choose the [backup policy](#) that has been created for this resource.

ENABLE BACKUP

Are you sure you want to enable backup for CISSEImage?

Select backup policy



USEastBackupVault

BackupWithValidation

DefaultPolicy

EnhancedPolicy

3. Click [OK](#).

Notes:

You can back up servers, images, hosts and Azure Files shares.

You can restore individual files/folders from Azure Files shares.

You can restore the entire contents of a server, hosts, images, etc.

You can validate your backups on resources (not Azure Files).

Day 2 - Lab 11



Day 2 - Lab 11.1 | Walkthrough



Enable Console Connect

Notes:

Before you can use Console Connect, you must enable it at the MSP level.

1. At the MSP level, navigate to [Settings > Integrations](#).

2. **Classic UI:** In the Console Connect tile, select [Disabled](#).

New UI: Scroll down to Console Connect, select the arrow to expand the settings sections, and then select [Disabled](#).

Console Connect ⓘ

Current status: [Disabled](#)

3. When prompted, confirm that you wish to enable Console Connect.

Enable it at the account level:

Before you can use Console Connect, you must enable it at the MSP level.

1. At the Account level, navigate to [Settings > Integrations](#).

2. **Classic UI:** In the Console Connect tile, select [Disabled](#).

New UI: Scroll down to Console Connect, select the arrow to expand the settings sections, and then select [Disabled](#).

CONSOLE CONNECT STATUS

Console Connect

On

Choose Intune groups, devices from there will be automatically added to Console Connect.

All Users x | x | v

Configure a confirmation prompt which appears on a desktop during initiating remote sessions.

☒ Session confirmation

Allow to manage your device?

All type of devices in acc-1 with Intune

Cancel

OK

Day 2 - Lab 11.1 | Walkthrough

Install Console Connect



1. Enter the following information:

Toggle Console Connect to [ON](#).

Choose Intune groups, devices that will be added.

Configure a prompt if needed.

Add session confirmation text.

CONSOLE CONNECT STATUS

Console Connect

On

Choose Intune groups, devices from there will be automatically added to Console Connect.

All Users x |

x

v

Configure a confirmation prompt which appears on a desktop during initiating remote sessions.

☒ Session confirmation

Allow [redacted] to manage your device?

All type of devices in acc-1 with Intune

Cancel

OK

Install the agent on an AVD session host.

1. At the Account level, locate the AVD host pool you wish to work with and select [Manage Hosts](#).
2. Locate the session host you wish to install agent on.
3. From the action menu, select [Console Connect > Install CC](#).

MANAGE CONSOLE CONNECT AGENT ON [redacted]

Are you sure you want to install Console Connect agent on [redacted]
nerdio.net?

Cancel

Confirm

Install the agent on a server.

1. At the Account level, navigate to [Servers](#).
2. Locate the server you wish to install agent on.
3. From the action menu, select [Console Connect > Install CC](#).
4. On the confirmation pop-up select [Confirm](#).

Install the agent on an Intune device.

1. At the Account level, [Intune > Devices](#).
2. Locate the Intune device you wish to install agent on.
3. From the action menu, select [Console Connect > Install CC](#).
4. On the confirmation pop-up select [Confirm](#).

Install the agent on a desktop image.

1. At the Account level, [Desktop Images](#).
2. Locate the desktop image you wish to install agent on.
3. From the action menu, select [Console Connect > Install CC](#).
4. On the confirmation pop-up select [Confirm](#).

Day 2 - Lab 11.2 | Walkthrough




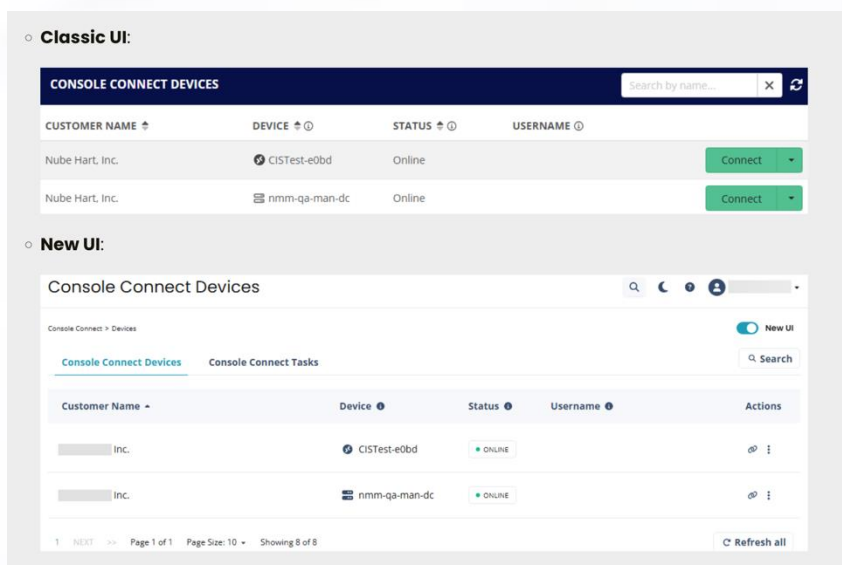
Connect to a session

Notes:

*You must enable Console Connect for an Account before you can use it.
The agents must be installed ahead of time, and devices be powered on.*

To connect to a session:

1. At the MSP level, [Console Connect](#) blade.
2. Locate the device you wish to connect to and select [Connect](#) or click on the .



1. Select [Interactive user session](#) and select [Connect](#).
2. On the confirmation pop-up select [Confirm](#).

CONSOLE CONNECT TO CISTEST-E0BD

☐ Toolbox

Initiate an unattended session to this target, providing you with a set of tools for diagnostics and problem resolution without interfering with potential user sessions.

☒ Interactive user session

New session

Cancel

Connect


Day 2 - Lab 11.2 | Walkthrough



Connect to a session

You can connect to an unattended session with the toolbox option.

You can connect to a session that also provides a list of powerful tools to help understand, diagnose, and resolve issues..

1. At the MSP level, [Console Connect](#) blade.
2. Locate the device you wish to connect to and select [Connect](#) or click on the  icon.
3. Select [Toolbox](#) and select [Connect](#).
4. Once the session is initiated, you may select the tool you would like to use.

