DGX Spark GB10 - EndPoint Onboarding Guide

Overview

This guide covers the provisioning process for NVIDIA DGX Spark / GB10 Grace Blackwell platform machines (e.g. MSI EdgeXpert MS-C931): first boot and baseline configuration of the preinstalled NVIDIA DGX OS, and onboarding the devices to NoTraffic security and management tooling (Microsoft Defender for Endpoint, ManageEngine Endpoint Central).

All units ship with NVIDIA DGX OS preinstalled. This guide assumes a factory-fresh system - no OS installation is required.

Workflow: only the initial setup (Section 1, first boot wizard) is performed locally on the device via the USB-C dock. All subsequent sections are performed **over SSH from the technician's computer**. Files (onboarding packages, agents) are downloaded on the technician's computer and copied to the device with `scp`. Connect with:

```
ssh "<user>@dgx-<department>-<##>"   # or the unit's IP address
```

For Entra ID (authd) users, quote the full username since it contains `@`, e.g. `ssh "yosefb.admin@notraffic.com@10.111.18.55"`

Deployment files - primary download location: the provisioning script, the Microsoft Defender ATP onboarding package, and the Endpoint Central UEMS ARM64 agent are stored in the IT SharePoint folder **NVIDIA DGX Spark**. Download the files from there first; only regenerate them from the Defender portal / Endpoint Central console (Sections 3.1 and 4.1) if the SharePoint copies are missing or outdated - and upload the fresh copies back to the folder.

Automated provisioning: the SSH-phase steps in this guide (Sections 1-4 device-side commands) are captured in the deployment script `dgx-spark-provision.sh` (in the NVIDIA DGX Spark SharePoint folder). Copy the script and both packages to the device, then run `sudo ./dgx-spark-provision.sh` - the script prompts for the owner's department and the unit's two-digit number, and builds the hostname `dgx-<department>-<##>` from them. The manual steps (Meraki reservation, Endpoint Central approval, 1Password entries) still apply and are printed by the script on completion.

> **Important platform limitation - read before starting:** The GB10 is an ARM64 (aarch64) platform. Microsoft Intune / Entra ID device registration for Linux is officially supported **only on x86/64 CPUs** (Ubuntu Desktop 24.04/26.04 LTS). The intune-portal and microsoft-identity-broker packages are not published for ARM64. **Full Entra ID device registration is NOT possible on these devices.** Section 2 covers the mandatory alternative: Entra ID user authentication via Canonical authd, plus device visibility via Defender for Endpoint.

Scope

- Applies to: all computers on the NVIDIA DGX Spark / GB10 Grace Blackwell platform (e.g. MSI EdgeXpert MS-C931, 128GB unified memory)
- OS: NVIDIA DGX OS 7.x (Ubuntu 24.04 LTS based, ARM64) - preinstalled
- Tooling: Entra ID user authentication via authd (mandatory), Microsoft Defender for Endpoint (Linux ARM64), ManageEngine Endpoint Central UEMS Linux agent (ARM64)

Computer Naming Convention

All DGX Spark machines follow this hostname convention:

`dgx-<department>-<two-digit number>`

- Example: `dgx-cto-01`, `dgx-cto-02`
- The department segment is the owning department (lowercase), and the two-digit number increments per unit within that department.

To set the computer name from the terminal:

```
sudo hostnamectl set-hostname dgx-cto-01
```

Prerequisites

- USB-C dock for initial setup (display, keyboard, and mouse connectivity)
- The provided power supply (use the original PSU that ships with the unit)
- Wired Ethernet on the NTS VLAN with internet access (no captive portal)
- Technician's computer on a network with SSH access to the device (for all post-setup steps and file transfers)
- Access to the NVIDIA DGX Spark SharePoint folder (provisioning script + deployment packages)
- Admin access to: Microsoft Entra admin center (app registration for authd), Microsoft Defender portal (security.microsoft.com), Endpoint Central console, Meraki dashboard (fixed IP assignments on the NTS VLAN)

- Endpoint Central server on build **2606.01 or later** (required for ARM64 Linux agent support)
- Access to the IT & Security vault in 1Password (local admin password entry `DGX Local Root Account`, and per-unit ntadmin entries)

1. First Boot and Baseline Configuration

Steps 1-4 are performed locally on the device (USB-C dock). From step 5 onward, work over SSH from the technician's computer.

1. Connect the unit to the USB-C dock and power it using the provided power supply.
2. Follow the first-time setup wizard: language, time zone (Asia/Jerusalem), keyboard layout, accept terms.
3. Create the local admin account per NoTraffic naming convention. Set the password to the value stored in the 1Password entry `DGX Local Root Account` (IT & Security vault) - the same local admin password is used on all DGX units.
4. Connect to the wired network (setup skips Wi-Fi selection if Ethernet is active). Allow up to 10 minutes for initial updates. Enable SSH if not already active, and note the device IP:

```
sudo systemctl enable --now ssh
ip -4 addr show
```

5. From the technician's computer, connect over SSH (all remaining steps in this guide):

```
ssh <local_admin>@<device_ip>
```

6. Set the hostname per the NoTraffic naming convention `dgx-<department>-<two-digit number>` (see "Computer Naming Convention" above). Example:

```
sudo hostnamectl set-hostname dgx-cto-01
```

7. Apply all updates:

```
sudo apt update
sudo apt upgrade -y
sudo reboot
```

   Reconnect over SSH after the reboot.
8. Verify GPU stack: `nvidia-smi` (note: "Memory-Usage: Not Supported" is expected on this iGPU platform).

1.1 Create the Local IT Sudo Account (MANDATORY - every unit)

Each machine must have a dedicated local IT administration account with sudo rights, separate from the end user's account. This account is the IT break-glass / support account for the device. The standard account name is `ntadmin`.

1. Over SSH, create the account:

```
sudo adduser ntadmin
```

When prompted, enter a strong, unique password (generate it in 1Password - do not reuse passwords between units).

2. Grant sudo rights:

```
sudo usermod -aG sudo ntadmin
```

3. Verify sudo access works:

```
su - ntadmin
sudo whoami
```

Expected output: `root`. Then `exit` back to your session.

4. **Document in 1Password** - in the IT & Security vault, create one entry per unit:
   - Item name: `DGX Spark - <hostname> - ntadmin` (e.g. `DGX Spark - dgx-cto-01 - ntadmin`)
   - Fields: username (`ntadmin`), password, hostname, IP address (reserved static IP, see Section 1.2), MAC address, site/location, serial number of the unit
   - Tag: `dgx-spark`

> ⚠ Do not skip the 1Password documentation step. The `ntadmin` account gets a **unique** password per unit and its own 1Password entry (unlike the local admin account from the setup wizard, which uses the shared `DGX Local Root Account` entry). A unit is not considered provisioned until its credentials are stored and verified in 1Password.

> Ongoing OS updates should be performed via the **DGX Dashboard**, which is the NVIDIA-recommended update path. Standard `apt` works but the Dashboard is the tested path.

1.2 Static IP Reservation on the NTS VLAN (MANDATORY - every unit)

Each machine must have a static IP on the NTS VLAN, implemented as a **fixed IP assignment** (DHCP reservation) in the Meraki dashboard. The device keeps DHCP enabled; the reservation guarantees it always receives the same address.

Step 1 - Get the MAC address (over SSH)

Retrieve the MAC of the interface currently holding the default route (the management/RJ45 interface on the NTS VLAN):

```
ip link show $(ip route show default | awk '{print $5}') | awk '/link\/ether/ {print $2}'
```

Alternatively run `ip a` and note the `link/ether` value of the interface holding the current IP.

⚠ **Grab the right NIC:** these machines expose multiple interfaces - the management RJ45 port plus the two ConnectX-7 QSFP ports (typically `enp1s0f*`), each with its own MAC. The reservation must use the MAC of the interface connected to the NTS VLAN, not a ConnectX port.

Step 2 - Create the fixed IP assignment in Meraki

1. On the technician's computer, sign in to the Meraki dashboard and go to where DHCP for the NTS VLAN is served:
   - MX appliance: **Security & SD-WAN > Configure > DHCP**
   - L3 switch: **Switching > Configure > Routing & DHCP** > open the NTS VLAN interface
2. In the NTS VLAN section, scroll to **Fixed IP assignments** and select **Add a fixed IP assignment**.
3. Fill in:
   - **Client name:** the hostname (e.g. `dgx-cto-01`)
   - **MAC address:** the value from Step 1
   - **LAN IP:** the reserved address for this unit (must be within the NTS VLAN subnet)
4. Save the configuration.

Step 3 - Renew the lease and verify (over SSH)

```
sudo dhclient -r && sudo dhclient
```

(or `sudo reboot`). Note: releasing the lease drops the SSH session - reconnect on the **reserved** IP. Verify with `ip -4 addr show` that the device now holds the reserved address, and record the IP and MAC in the unit's 1Password entry (Section 1.1).

Keep the numbering predictable: map the unit number to the host octet (e.g. `dgx-cto-01` → `x.x.x.11`, `dgx-cto-02` → `x.x.x.12`). Record the scheme here once the range is allocated.

2. Entra ID User Authentication via authd (MANDATORY - every unit)

Full Entra ID / Intune device registration is not possible on ARM64 (see the platform limitation above). The following table summarizes what applies on this platform:

Capability	Status on GB10 (ARM64)	Notes
Intune enrollment / Entra device registration	NOT SUPPORTED	intune-portal + identity broker are x86/64 only

Entra ID user login to the OS (authd)	MANDATORY	Canonical authd + MS Entra ID broker snap; user auth only, no device object compliance
Device visibility in Defender portal	SUPPORTED	Defender onboarding creates a device record in Microsoft Defender XDR

Entra ID user authentication via authd is **mandatory on every unit**. Users log in to the device with their NoTraffic Entra ID credentials (including MFA). Note this does **not** register the device in Entra ID - device-level visibility comes from Defender onboarding (Section 3).

> **PPA required:** DGX OS is Ubuntu 24.04 based, and on 24.04 authd is not in the default package archive - running `apt install authd` without the PPA fails with "Unable to locate package authd". Add the stable authd PPA first (step 1 below).

App Registration Details (all units)

A single Entra ID app registration serves all DGX Spark units. Access is restricted via app assignment (see the access control panel below).

Field	Value
Enterprise Application name	`Azure OIDC linux - DGX - CTO Team`
Application (client) ID	`1a70be90-d421-4270-87ab-0a751a5106d6`
Directory (tenant) ID	`ae0cceeb-0299-4a8c-875b-ac9160f7b8a7`
Issuer URL	`https://login.microsoftonline.com/ae0cceeb-0299-4a8c-875b-ac9160f7b8a7/v2.0`
Login access group (non-sudo)	`apps_azure_oidc_linux-dgx-ctoteam` (dynamic security group)
Sudo access groups	`linux-sudo` and `linux_azure_oidc_linux-dgx-ctoteam` (see Section 2.1)

Access control: the Enterprise Application has **"Assignment required" = Yes**. Only members of the **dynamic security group** `apps_azure_oidc_linux-dgx-ctoteam` (assigned to the app) can authenticate to the DGX machines - this grants standard (non-sudo) login. Membership is rule-based (dynamic); users are added/removed automatically by the group's membership rule rather than manually. Sudo rights are granted separately (Section 2.1). Assignment changes take effect at the user's next fresh Entra authentication.

Installation and Configuration Steps (over SSH)

1. Add the authd stable PPA:

```
sudo add-apt-repository ppa:ubuntu-enterprise-desktop/authd
sudo apt update
```

2. Install authd and the Entra ID broker:

```
sudo apt install -y authd
sudo snap install authd-msentraid
```

3. Configure the broker - edit `/var/snap/authd-msentraid/current/broker.conf` and set:

```
[oidc]
issuer = https://login.microsoftonline.com/ae0cceeb-0299-4a8c-875b-ac9160f7b8a7/v2.0
client_id = 1a70be90-d421-4270-87ab-0a751a5106d6

[users]
allowed_users = ALL
ssh_allowed_suffixes = @notraffic.com,@notraffic.tech
```

`allowed_users = ALL` is required (the commented-out default is `OWNER`, which only allows the first user who ever logged in and causes "access denied" for everyone else). ALL is safe here because access is enforced by the Enterprise App assignment. `ssh_allowed_suffixes` enables SSH logins for Entra users - it takes a comma-separated list of allowed username suffixes.

4. Enable PAM keyboard-interactive authentication and TTY allocation for SSH - required for authd to display the device-code login prompt over SSH:

```
printf "UsePAM yes\nKbdInteractiveAuthentication yes\nPermitTTY yes\n" | sudo tee
/etc/ssh/sshd_config.d/authd.conf
sudo systemctl restart ssh
sudo sshd -T | grep -Ei "usepam|kbdinteractive|permittty"
```

All three must return `yes`. If `kbdinteractiveauthentication` or `permittty` shows `no`, another drop-in is overriding it - check with `sudo grep -ri "KbdInteractiveAuthentication\|PermitTTY" /etc/ssh/` and rename the authd.conf file to sort alphabetically before the conflicting file (e.g. `01-authd.conf`).

> ⚠ **PermitTTY is required:** without it, sshd cannot open a TTY for the PAM conversation and authd fails with "failed to open pam tty" - the SSH connection is refused for Entra ID users. Local accounts (ntadmin, local admin) are unaffected since they don't go through the PAM/authd flow.

5. Register the broker with authd and restart the services:

```
sudo mkdir -p /etc/authd/brokers.d/
sudo cp /snap/authd-msentraid/current/conf/authd/msentraid.conf /etc/authd/brokers.d/
sudo systemctl restart authd
sudo snap restart authd-msentraid
```

6. Test login with a NoTraffic Entra ID account that is a member of `apps_azure_oidc_linux-dgx-ctoteam`. SSH works as a first login - no prior console login required. The user will see a Microsoft device-code prompt in the terminal:

```
ssh "user@notraffic.com@<device_ip>"
```

   They open the URL (microsoft.com/devicelogin) in any browser, enter the code, complete MFA, and the SSH session opens. On first login authd will prompt them to set a local password - this is by design (see note below). Also verify a user **outside** the group is rejected.

> **Local password prompt on first login:** after the Entra device-code flow, authd prompts the user to set a local machine password. This is expected behaviour - the local password is used for offline scenarios (screen unlock, sudo prompts, network unavailable) and is scoped to that machine only. It is not the user's Entra password and works nowhere else. The trust anchor remains Entra: account state, group membership and app assignment are all enforced on every fresh online authentication.

> **Troubleshooting - "can't refresh token" after a client_id change:** users who logged in under a previous app registration have a cached refresh token bound to the old app; Entra correctly refuses to refresh it against the new client_id. Fix (run as the local admin):
>
> ```
> sudo find /var/snap/authd-msentraid/ -type f \( -iname "*token*" -o -iname "*cache*" \) 2>/dev/null
> sudo rm -rf /var/snap/authd-msentraid/current/cache/*
> sudo snap restart authd-msentraid
> sudo systemctl restart authd
> ```
>
> If authd still attempts a silent refresh, also check for the user's record under `/var/lib/authd/` and remove it - it is recreated cleanly on the next login, and the user's home directory is unaffected.

2.1 Sudo Rights via Entra ID Groups

Standard (non-sudo) login access is controlled by the app assignment group `apps_azure_oidc_linux-dgx-ctoteam`. Sudo is granted through Entra ID group membership using either of two mechanisms:

Option A - linux-sudo (authd prefix mapping)

authd maps Entra ID groups prefixed with `linux-` (hyphen) to local machine groups: membership in the Entra ID group `linux-sudo` grants membership in the local `sudo` group on login. No machine-side configuration is required.

Option B - linux_azure_oidc_linux-dgx-ctoteam (sudoers rule)

The Entra ID group `linux_azure_oidc_linux-dgx-ctoteam` (note: `linux_` with an underscore does NOT trigger the authd prefix mapping) comes through as a regular remote group - a local group of the same name is created on the user's login. Sudo is granted to it via a sudoers drop-in on each machine:

```
echo '%linux_azure_oidc_linux-dgx-ctoteam ALL=(ALL:ALL) ALL' | sudo tee /etc/sudoers.d/dgx-ctoteam-sudo
sudo chmod 440 /etc/sudoers.d/dgx-ctoteam-sudo
sudo visudo -c
```

Requirements for both options

1. Sudo users must also be matched by `apps_azure_oidc_linux-dgx-ctoteam` to be able to log in at all - the sudo groups elevate privileges but do not grant login.
2. On the app registration, the delegated Microsoft Graph permission `GroupMember.Read.All` must be added with admin consent granted - without it, the broker cannot read group memberships and no groups are mapped.
3. Verify after the user's next login:

   ```
   groups <user>
   ```

   The output should include `sudo` (Option A) or `linux_azure_oidc_linux-dgx-ctoteam` (Option B).

⚠ **Scope:** membership in either sudo group grants sudo on **every machine using this app registration** (Option B additionally requires the sudoers drop-in to be present on the machine, which the provisioning script deploys). Manage membership accordingly. Group changes take effect on the user's **next login**, not immediately.

The `linux-` prefix mapping works for other privileges too: an Entra ID group named `linux-<group>` maps to the local group `<group>` (e.g. `linux-docker` → local

`docker` group). Non-prefixed Entra ID groups are created as regular remote groups (lowercased).

Known interoperability issues exist between authd users and GNOME keyring flows - validate the full login experience on the first unit before rolling out to the remaining units.

3. Install Microsoft Defender for Endpoint (Linux ARM64)

Defender for Endpoint supports ARM64 Linux servers in GA (agent version 101.25022.0004 and later). DGX OS is an Ubuntu 24.04 derivative - Defender can be installed on derived distributions meeting kernel requirements, but this is a best-effort support scenario.

The method used is the **installer script + onboarding package**: the public `mde_installer.sh` script installs the agent, and the tenant-specific onboarding package onboards the device to the NoTraffic Defender tenant. The onboarding package is reused for all DGX units.

Microsoft also offers a "Defender deployment tool" single-package method, but at the time of writing it is not available for Linux in our tenant (Windows only). Revisit once the Linux deployment tool reaches our tenant.

3.1 Get the Onboarding Package (technician's computer)

Primary location: download `GatewayWindowsDefenderATPOnboardingPackage.zip` from the **NVIDIA DGX Spark** SharePoint folder. The package is tenant-wide and reusable on all units. Only regenerate it from the Defender portal (steps below) if the SharePoint copy is missing or no longer valid - and upload the fresh copy back to the folder.

To regenerate the package from the Defender portal:

1. On the technician's computer, sign in to the Microsoft Defender portal: security.microsoft.com.
2. Go to **System > Settings > Endpoints > Device management > Onboarding**.
3. In the operating system drop-down, select **Linux Server** (NOT a Windows option - a package that extracts a `.onboarding` file is the Windows package and cannot be used on Linux); as the deployment method, select **Local Script**.
4. Select **Download onboarding package**. Verify the package is correct before use: `unzip -l <package>.zip` must show `MicrosoftDefenderATPOnboardingLinuxServer.py`.

> The package is generated behind the Defender portal login and is tenant-specific - it cannot be downloaded with curl/wget from a public URL.

3.2 Copy the Package to the DGX (scp from technician's computer)

Copy the package from the technician's computer to the Desktop folder of the user you connect with on the DGX. Example (Entra ID user via authd - note the quoted username, since authd usernames contain `@`):

```
scp .\GatewayWindowsDefenderATPOnboardingPackage.zip
"yosefb.admin@notraffic.com@10.111.18.55:~/Desktop/"
```

- Replace the username with the account you connect with over SSH, and the IP with the unit's address or hostname.
- Copy and run the installation as the **same user** - copying as one user and installing as another leads to "cannot find or open" errors, since `~/Desktop` resolves per user.
- Linux paths are case-sensitive: the folder is `~/Desktop` (capital D). If it does not exist yet on a fresh account: `ssh "<user>@<host>" 'mkdir -p ~/Desktop'`

3.3 Install and Onboard (over SSH)

1. SSH into the DGX, then download and run the installer script:

```
curl -o mde_installer.sh https://raw.githubusercontent.com/microsoft/mdatp-
xplat/master/linux/installation/mde_installer.sh
chmod +x mde_installer.sh
sudo ./mde_installer.sh --install --channel prod
```

2. Onboard the device using the onboarding package:

```
unzip GatewayWindowsDefenderATPOnboardingPackage.zip
sudo python3 MicrosoftDefenderATPOnboardingLinuxServer.py
```

3. Verify health:

```
mdatp health --field healthy
mdatp health --field licensed
```

   Both must return `true`.

4. Confirm the device appears in the Defender portal under **Assets > Devices** (may take 5-20 minutes on first onboarding).

> ⚠ **Performance exclusions:** These are AI workstations - real-time scanning of model files and training datasets can significantly impact performance. After onboarding, add antivirus exclusions for AI working directories (e.g. model/dataset paths, `/home/*/models`) via Defender policy. Coordinate with the users before finalizing exclusions.

4. Install Endpoint Central UEMS Agent (Linux ARM64)

ARM64 Linux agents are supported from Endpoint Central build 2606.01. Supported feature set on ARM64 is limited to: Configurations, Inventory Management, Agent SoM policy, and Tools. **Linux patch management and software deployment are NOT available for ARM64 agents** - patching stays on the DGX Dashboard / apt.

4.1 Get the Agent (technician's computer)

> **Primary location:** download the UEMS ARM64 agent ZIP (e.g. `DefaultRemoteOffice_UEMSLinuxAgent_ARM64.zip`) from the **NVIDIA DGX Spark** SharePoint folder. Only download a fresh copy from the Endpoint Central console (steps below) if the SharePoint copy is missing, the target unit belongs to a different remote office, or the agent version is outdated - and upload the fresh copy back to the folder.

To download a fresh agent from the console:

1. On the technician's computer, sign in to the Endpoint Central console (server build 2606.01 or later - check the build number at the top right of the console).
2. Go to **Agent > Computers > Download Agent**.
3. Select Platform: **Linux**, Processor: **ARM64**, and the correct remote office / LAN.
4. Download the agent ZIP - the filename includes the remote office, e.g. `DefaultRemoteOffice_UEMSLinuxAgent_ARM64.zip`.

> Download the agent through the console in a browser. Emailed or copied download links contain embedded, expiring API keys and typically return an HTML page instead of the ZIP when fetched with wget/curl (unzip then fails with "End-of-central-directory signature not found"). If a direct download on the device is ever needed, verify the result with `file <name>.zip` before unzipping.

4.2 Copy the Agent to the DGX (scp from technician's computer)

```
scp .\DefaultRemoteOffice_UEMSLinuxAgent_ARM64.zip
"yosefb.admin@notraffic.com@10.111.18.55:~/Desktop/"
```

Replace the username, IP, and remote-office filename as appropriate (same rules as Section 3.2).

4.3 Install (over SSH)

1. SSH into the DGX, extract, make the installer executable, and run it:

```
cd ~/Desktop
unzip DefaultRemoteOffice_UEMSLinuxAgent_ARM64.zip
# Extracts: UEMS_LinuxAgent_ARM64.bin, serverinfo.json, LINUX_README.txt
chmod +x UEMS_LinuxAgent_ARM64.bin
sudo ./UEMS_LinuxAgent_ARM64.bin
```

2. The agent installs to `/usr/local/manageengine/uems_agent/` by default.

> ⚠ **Required - chmod before running:** the .bin must be made executable with `chmod +x UEMS_LinuxAgent_ARM64.bin` before running it. unzip does not preserve the execute permission, and without it `sudo ./UEMS_LinuxAgent_ARM64.bin` fails with the misleading error "command not found". The `serverinfo.json` file must remain in the same directory as the .bin when running the installer.

4.4 Approve the Machine in the Endpoint Central Console

1. On the technician's computer, open the Endpoint Central admin console.
2. Newly installed agents land in the pending-approval queue (Scope of Management). Go to **Agent > Computers** and locate the new machine - machines awaiting approval are flagged for action.
3. **Approve** the machine to bring it under management. Until approved, the agent will not report inventory or receive configurations.
4. After approval, verify the device appears under the correct remote office and reports inventory within a few minutes. If it does not appear at all, check `/usr/local/manageengine/uems_agent/logs/` on the device (start with `httpaccess0.log`) for connectivity errors.

5. Per-Unit Verification Checklist

- [ ] DGX OS fully updated (DGX Dashboard shows current)
- [ ] Hostname set per convention (dgx-<department>-<##>), recorded in inventory
- [ ] Local admin password set from 1Password entry "DGX Local Root Account"
- [ ] ntadmin sudo account created, sudo verified (sudo whoami = root)
- [ ] Unique ntadmin password generated and entry created in 1Password (username, password, hostname, IP, MAC, serial)
- [ ] Static IP: MAC recorded, fixed IP assignment created in Meraki on the NTS VLAN, lease renewed, reserved IP verified
- [ ] sshd authd.conf written (UsePAM yes, KbdInteractiveAuthentication yes, PermitTTY yes), sshd -T confirms all three, SSH restarted
- [ ] authd installed (PPA added), allowed_users=ALL + ssh_allowed_suffixes set, broker registered, services restarted
- [ ] Entra ID SSH login tested for an apps_azure_oidc_linux-dgx-ctoteam member (device-code flow, MFA, local password set), non-member rejected
- [ ] Sudo groups verified: linux-sudo mapping and/or dgx-ctoteam sudoers drop-in in place (visudo -c passes)
- [ ] nvidia-smi returns GPU status
- [ ] Defender: mdatp healthy=true, licensed=true, visible in Defender portal
- [ ] Defender AV exclusions for AI workload paths applied
- [ ] Endpoint Central agent installed, machine approved in console, reporting inventory

References

- NVIDIA DGX Spark - SharePoint Deployment Files Folder

- DGX Spark - Initial Setup / First Boot
- Canonical authd Documentation
- authd - Group and Privilege Management
- authd Stable PPA (Launchpad)
- Defender for Endpoint on Linux - Installer Script Deployment
- Defender for Endpoint on Linux - Prerequisites
- Intune Linux Enrollment (x86/64 only)
- Endpoint Central - Linux Agent Installation
- Meraki - Configuring DHCP Services (Fixed IP Assignments)
- MSI EdgeXpert MS-C931 Product Page