Offline installation.
Every stage, explained.

Visual customer and partner handbook for One Ticket Less: VMware / ESXi, Microsoft Hyper-V, Huawei Cloud x86 and Huawei FusionCompute x86.

What the visuals mean
SCREENSHOT: a real earlier OTL/VMware training capture. Host identifiers are excluded by cropping.
REFERENCE ILLUSTRATION: a labelled configuration diagram, not a screenshot or proof of native-host testing.
Hyper-V/Huawei host walkthroughs use these where captures are unavailable.

Edition 2.0 | 9 November 2026 | Includes the complete 16-section Linux command and operations reference as an appendix.

Fictional training company: Northstar Services. Example address: 192.0.2.50 (replace it). Captures may show an earlier release, a seven-day training licence, legacy wording or different dates. They demonstrate the action, not the validity of your licence.

Your visual roadmap

Choose a host chapter, then follow all Shared chapters. The final appendix contains the detailed Linux commands and operational checks.

01 Choose your installation path	3
02 Request and verify the package	4
03 VMware 1 - select the OVA	5
04 VMware 2 - choose storage	6
05 VMware 3 - network and deployment options	7
06 VMware 4 - review and finish	8
07 Hyper-V 1 - prepare the VHDX	9
08 Hyper-V 2 - optional helper	10
09 Hyper-V 3 - manual wizard	11
10 Hyper-V 4 - firmware and first start	12
11 Huawei Cloud 1 - request the right format	13
12 Huawei Cloud 2 - image service to ECS	14
13 FusionCompute 1 - separate VHD package	15
14 FusionCompute 2 - qualify and boot	16
15 Shared 1 - verify Linux startup	17
16 Shared 2 - trusted HTTPS and setup key	18
17 Shared 3 - create company and owner	19
18 Shared 4 - find Licensing	20
19 Shared 5 - download installation request	21
20 Shared 6 - import and verify activation	22
21 Shared 7 - locations, users and workflow	23
22 Shared 8 - sign-in, mail and gate passes	24
23 Finish - backup, reboot and acceptance	25

CUSTOMER DEPLOYMENT GUIDE / 01

Choose your installation path

REFERENCE ILLUSTRATION - not a captured host screen

Download -> import -> Linux -> browser -> licence	Your selection
VMware / ESXi	OVA -> OVF deployment wizard -> VM console
Microsoft Hyper-V	VHDX ZIP -> Generation 2 VM -> VM console
Huawei Cloud x86	QCOW2 ZIP -> approved IMS/image import -> ECS console
Huawei FusionCompute x86	VHD ZIP -> qualified import workflow -> VM console
All four	Stable IP -> HTTPS trust -> owner -> signed licence -> company configuration

Read this first

1. Follow only the host chapter that matches your platform. Then follow the shared Linux/browser chapters in order.

2. Obtain the authenticated package hash and the package-specific instructions. Keep an untouched original archive.

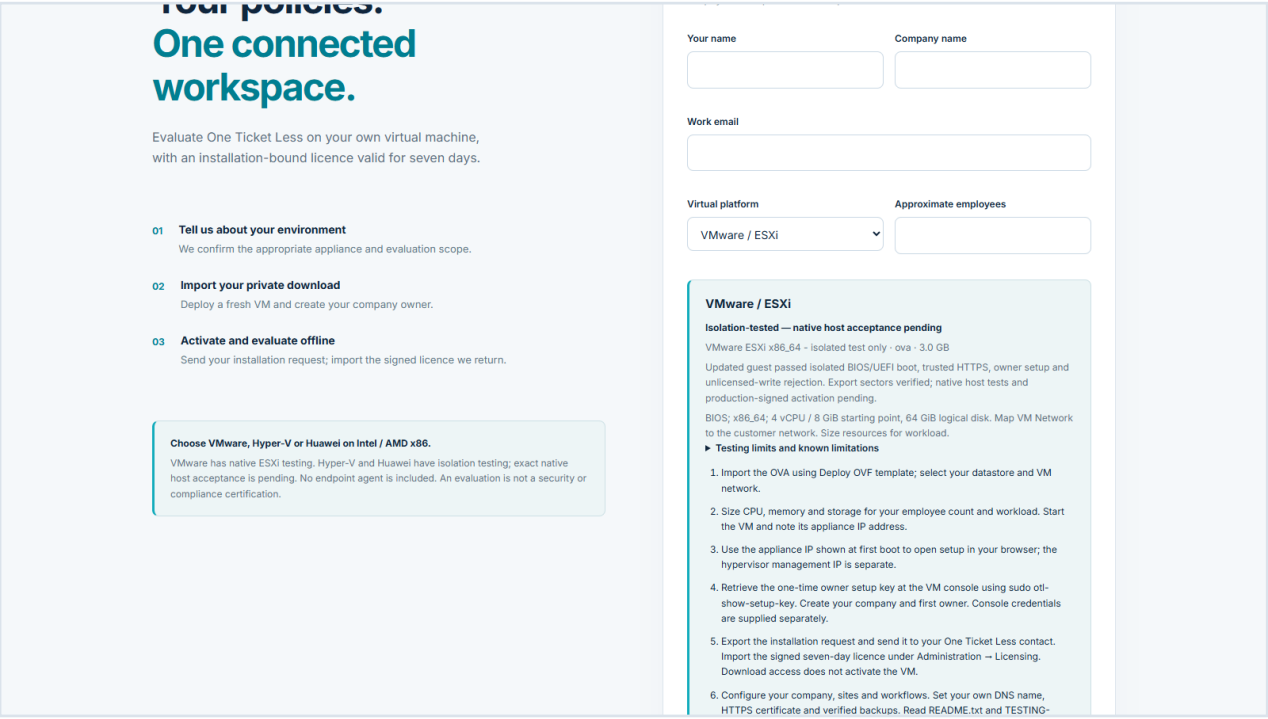
3. Agree CPU, RAM, disk, network, time, certificate and backup arrangements. Size for workload; do not copy a training system's capacity blindly.

4. For 30 days offline, request an explicitly dated 30-day licence. Downloading the appliance is not activation.

All formats passed isolated tests. Exact final native-host acceptance remains a separate gate; Huawei has no native-host validation here. The current kernel findings remain documented. This handbook does not turn an illustrated step into certification.

CUSTOMER DEPLOYMENT GUIDE / 02

Request and verify the package



SCREENSHOT - Actual website platform selector from the earlier customer walkthrough.

1. Open the offline trial/request section of oneticketless.com. Enter your business details and choose the correct platform.

2. For a paid 30-day arrangement, tell the vendor the required term and technician allowance; do not assume the seven-day evaluation selection grants a month.

3. After approval, use the authorised download link. Observe its expiry and retain the installation instructions/checksum.

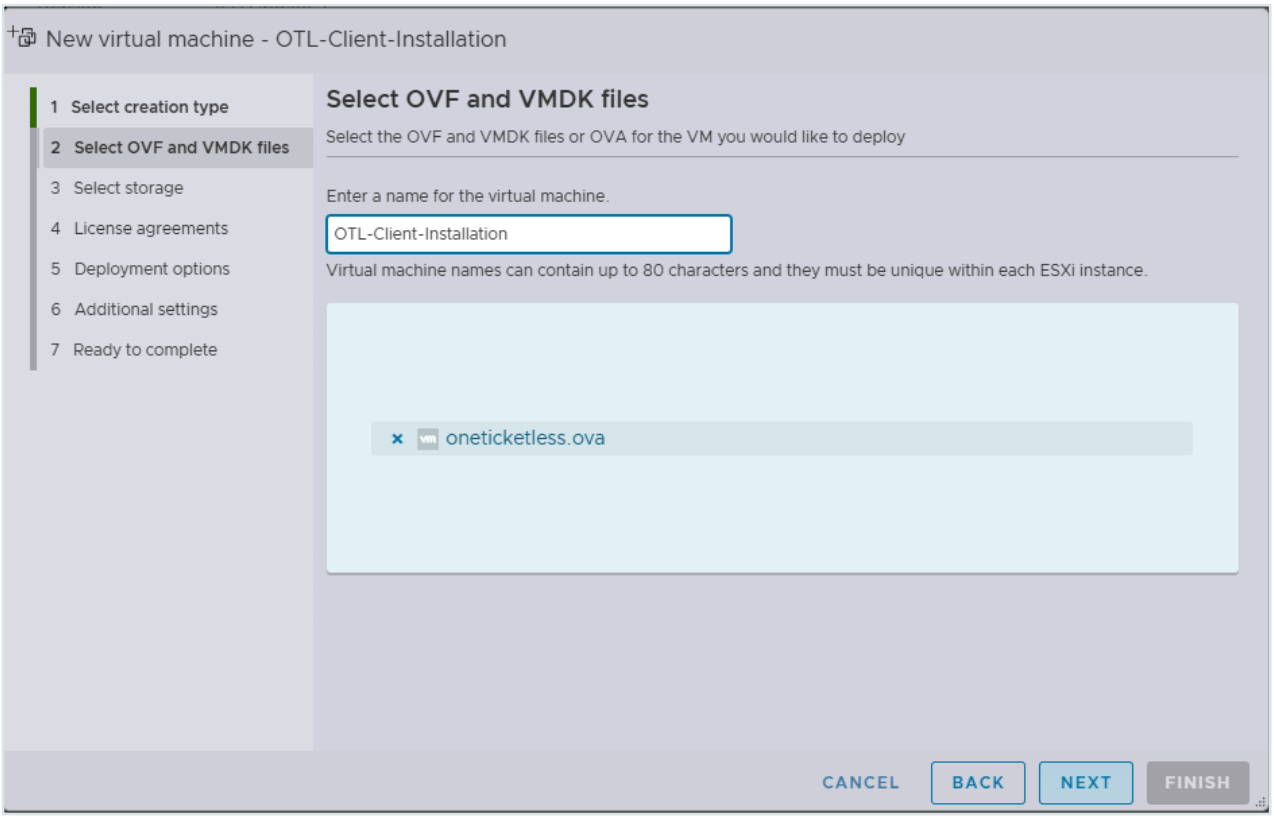
4. On Linux, run sha256sum against the actual archive; on Windows use Get-FileHash. Compare with the authenticated vendor value before extracting or importing.

```
sha256sum /path/to/OneTicketLess-release.ova
# Windows PowerShell alternative:
Get-FileHash -Algorithm SHA256 "C:\Downloads\release.zip"
```

Before moving on: The package platform and complete SHA-256 match. If not, stop and re-download.

CUSTOMER DEPLOYMENT GUIDE / 03

VMware 1 - select the OVA



SCREENSHOT - Actual ESXi import wizard, cropped to the deployment dialogue.

1. In the ESXi Host Client, choose Create/Register VM and deployment from OVF/OVA. vCenter may label the action Deploy OVF Template.

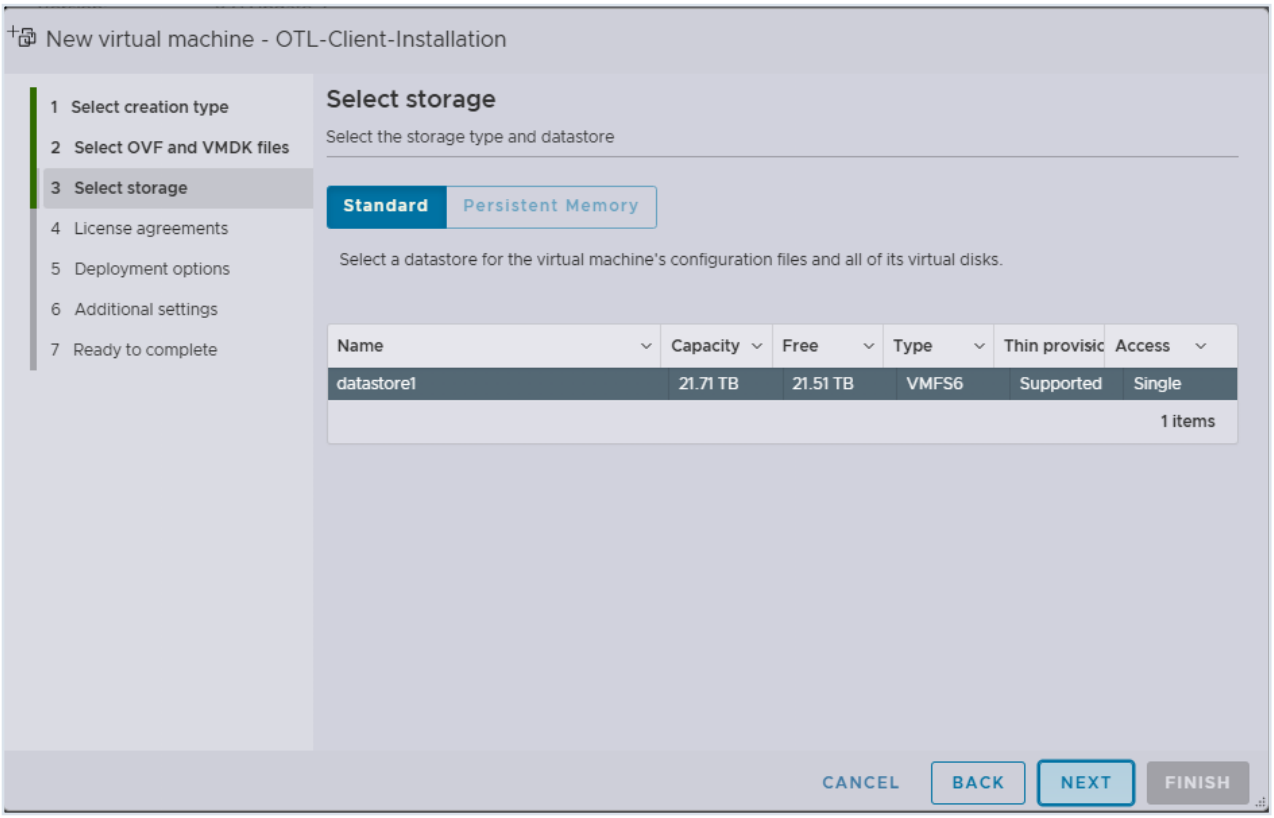
2. Enter a unique VM name and select the delivered .ova. If a supplied extraction includes OVF/VMDK, use only the matching files from that package.

3. Wait for the wizard to read the definition, then continue. The OVA already contains an operating system and application; no Ubuntu ISO install is needed.

Before moving on: A new VM is being created. No existing customer disk or VM is selected for overwrite.

CUSTOMER DEPLOYMENT GUIDE / 04

VMware 2 - choose storage



SCREENSHOT - Actual datastore selection; displayed capacity is only a training example.

1. Select an approved datastore with capacity for growth, the virtual disk and your backup/restore policy.

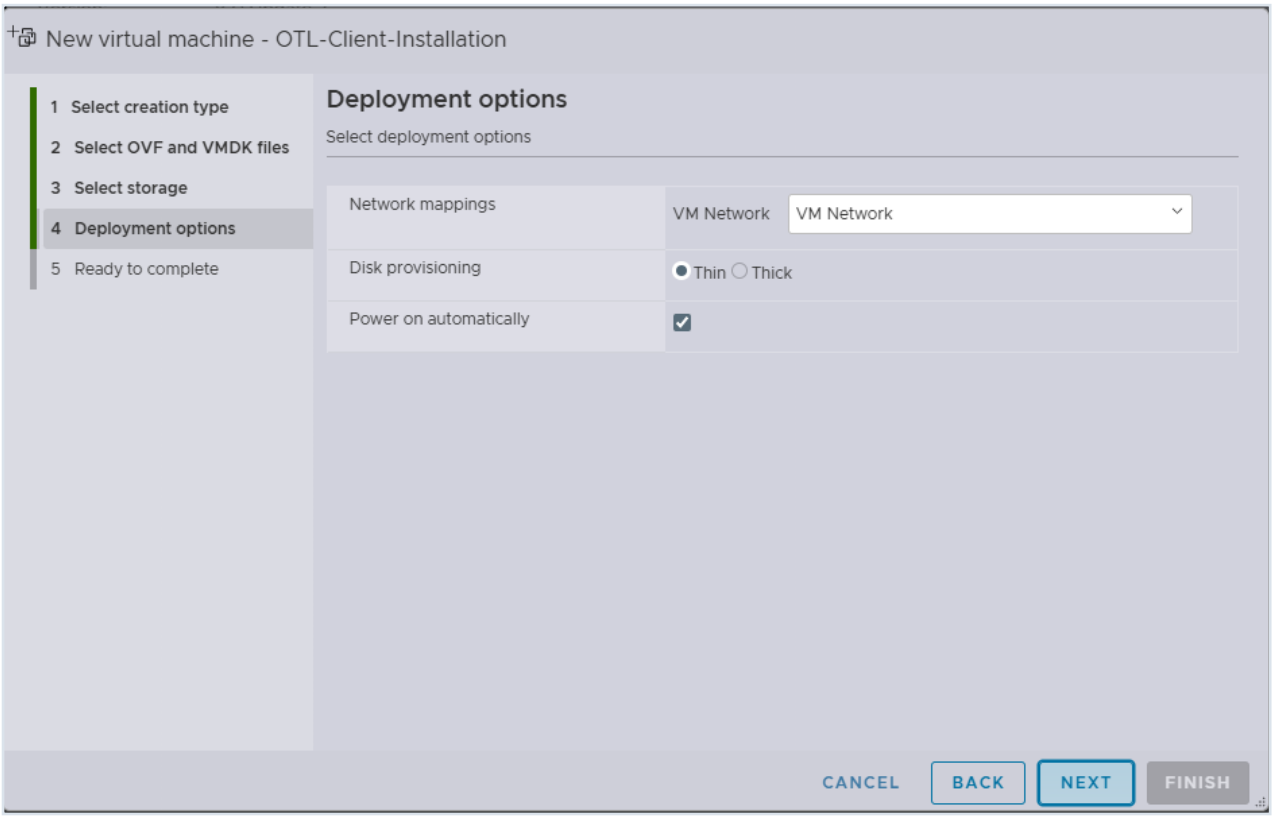
2. Check the reference logical disk size in the delivery notes. Thin provisioning saves initial space but is not free capacity.

3. Do not choose storage solely because it fits today's compressed download. Continue after confirming the correct datastore.

Before moving on: The datastore and storage policy are suitable for the agreed customer workload.

CUSTOMER DEPLOYMENT GUIDE / 05

VMware 3 - network and deployment options



SCREENSHOT - Actual deployment-options screen. Options vary by ESXi version.

1. Map the virtual network to your real port group/VLAN. VM Network is only the training label.

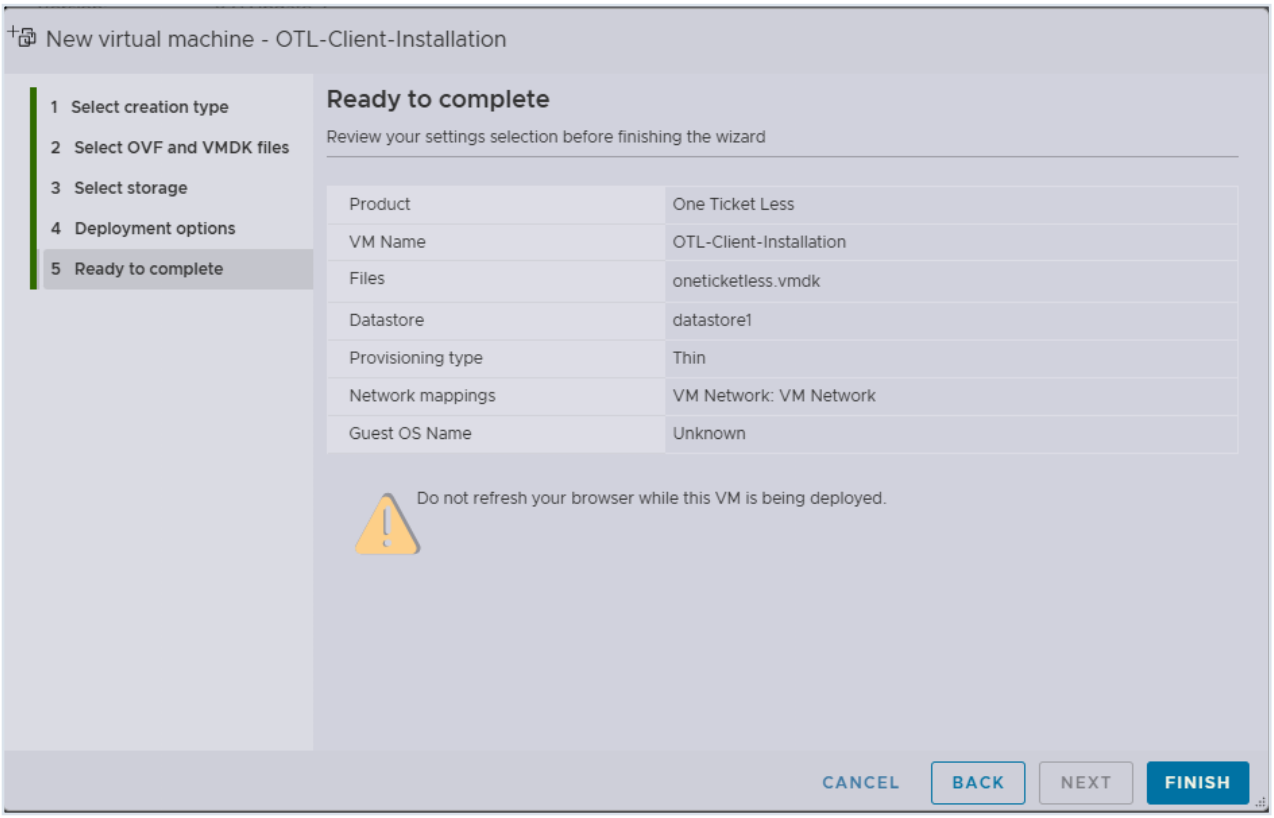
2. Choose the approved disk allocation. Review power-on behaviour and change only settings supported by your release instructions.

3. Confirm DHCP is available or plan a console-based static address. Ensure the NIC will connect at startup.

> **Before moving on:** The mapped network is the customer LAN, not the hypervisor-management address or an isolated switch without the required connectivity.

CUSTOMER DEPLOYMENT GUIDE / 06

VMware 4 - review and finish



SCREENSHOT - Actual final review before importing the training VM.

1. Check VM name, package, datastore, network mapping and virtual hardware. Confirm it is a new deployment.

2. Finish and wait for upload/import completion. Do not close or refresh a browser that is actively uploading the appliance.

3. Open the VM console, review CPU/RAM/NIC settings, then power on if not started automatically. Allow image loading to complete.

> **Before moving on:** The VM reaches the Linux console and displays an OTL portal address. Continue at the shared first-boot chapter.

CUSTOMER DEPLOYMENT GUIDE / 07

Hyper-V 1 - prepare the VHDX

REFERENCE ILLUSTRATION - not a captured host screen

Hyper-V delivery preparation	Your selection
Archive	Hyper-V ZIP only
Disk	Extracted oneticketless.vhdx
Preserve	Untouched delivery copy plus checksum
Destination	New VM folder on approved storage
Host	Hyper-V role/management available; authorised operator

1. Verify the ZIP checksum and extract it. Do not try to import the ZIP as a Hyper-V exported VM; this delivery is a virtual hard disk plus instructions.

2. Choose a unique VM name and a fresh storage folder. Retain the original VHDX as the delivery source.

3. Open Hyper-V Manager and connect to your authorised host. Confirm its virtual switch reaches the required LAN/VLAN.

Two supported ways through this guide

Use the supplied PowerShell helper in the next chapter, or use New > Virtual Machine and follow the illustrated settings on the following pages. Both attach an existing operating-system disk. Do not create an empty OS disk or choose an installer ISO.

Before moving on: The existing VHDX is intact, and the intended virtual switch is identified.

CUSTOMER DEPLOYMENT GUIDE / 08

Hyper-V 2 - optional helper

Run the following in an elevated PowerShell window on the **Hyper-V host**, from the directory containing the delivered Create-HyperV.ps1. Do not run it inside the Linux guest.

```
Get-VMSwitch
.\Create-HyperV.ps1 `
  -VhdxPath "D:\OTL-Download\oneticketless.vhdx" `
  -StorageRoot "D:\VirtualMachines" `
  -SwitchName "Company-LAN" `
  -VMName "OneTicketLess" -EnableSecureBoot -WhatIf
```

1. Replace both paths and the switch name. First review -WhatIf output; it should target a new VM folder.

2. Run the same command without -WhatIf after review. The helper copies/verifies the disk, creates Generation 2 and selects the Microsoft UEFI CA template when requested.

3. The helper does not start the VM. Open its settings and review sizing, switch, boot disk and firmware before starting.

4. If a name/folder exists, use a genuinely new name/folder. Do not delete existing machines to force the helper through.

REFERENCE ILLUSTRATION - not a captured host screen

Result to expect	Your selection
VM generation	2
Disk	Copy of delivered VHDX, attached to SCSI
Secure Boot, if enabled	Microsoft UEFI Certificate Authority
First action after review	Connect to console; Start

CUSTOMER DEPLOYMENT GUIDE / 09

Hyper-V 3 - manual wizard

REFERENCE ILLUSTRATION - not a captured host screen

New Virtual Machine wizard	Your selection
Action	New > Virtual Machine
Name and location	OneTicketLess; approved new VM directory
Generation	Generation 2
Memory	Agreed workload sizing; reference 8 GB
Networking	Existing company virtual switch
Virtual hard disk	Use an existing virtual hard disk -> copied VHDX

1. Choose New > Virtual Machine. Enter a unique name and a storage path with sufficient space.

2. Select Generation 2. The supplied VHDX is not an installation ISO.

3. Assign startup memory according to the deployment plan. The shipped helper uses static memory; use a tested configuration.

4. Choose the approved virtual switch. For server use, do not assume a laptop's Default Switch provides a stable address.

5. Choose Use an existing virtual hard disk and browse to the copied VHDX. Finish only after reviewing the summary.

Before moving on: The disk path points to your VM copy, not the protected original delivery copy.

Hyper-V 4 - firmware and first start

REFERENCE ILLUSTRATION - not a captured host screen

VM Settings before power-on	Your selection
Processor	Agreed vCPU count; reference 4
SCSI controller	Delivered VHDX attached and selected as boot disk
Network adapter	Correct switch and VLAN
Security / Secure Boot	If enabled: Microsoft UEFI Certificate Authority
Console	Connect, then Start

1. Open Settings for the new VM. Review processors, memory, disk attachment and network.

2. For Linux Secure Boot, select the Microsoft UEFI Certificate Authority template, not the Windows-only template. Follow the release's tested firmware configuration.

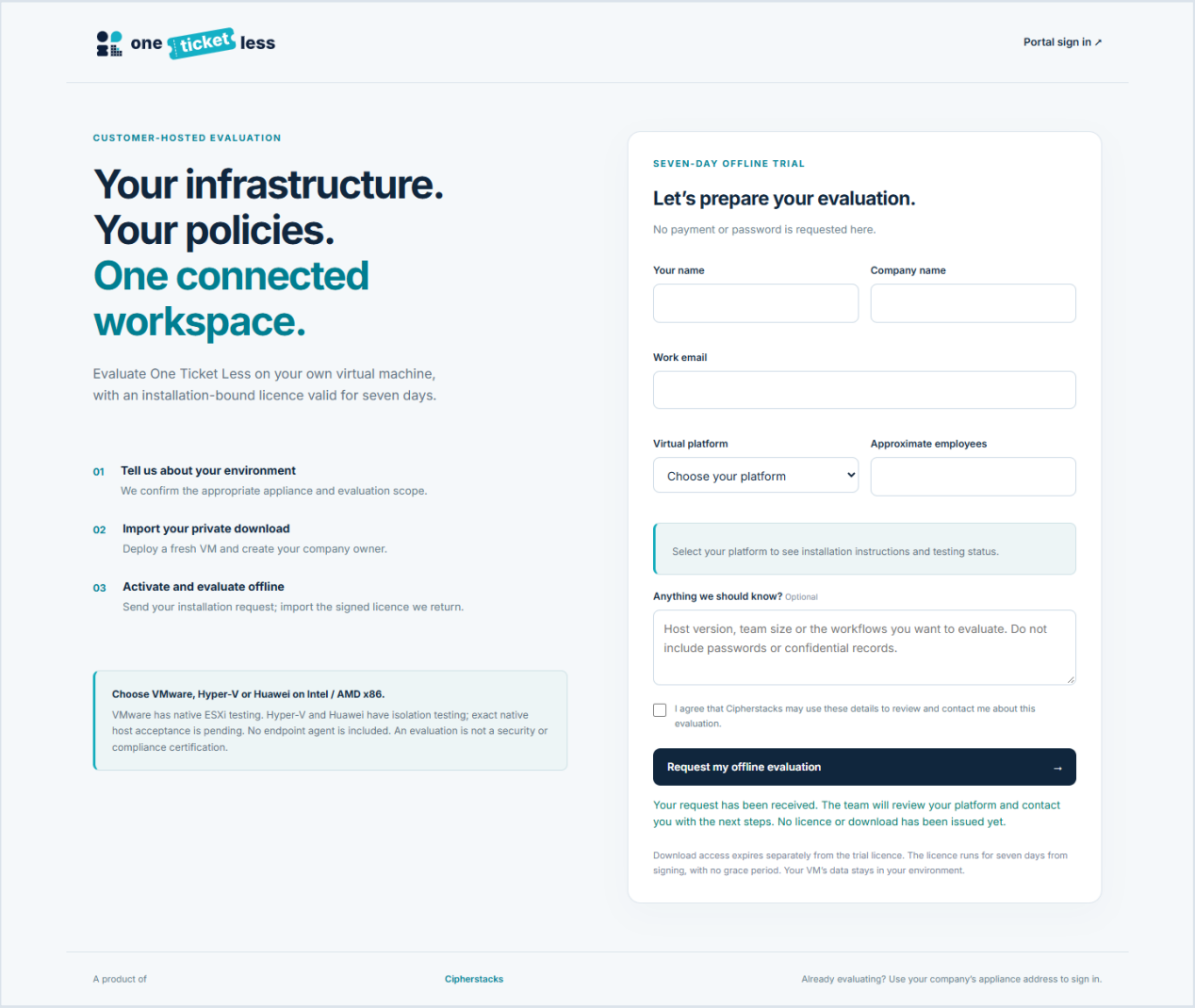
3. Connect to the VM console and start it. If boot fails, record the exact firmware message rather than switching controllers randomly.

4. After Linux boots, use its displayed portal IP. Verify DHCP and guest services; missing host-side IP display alone does not prove the guest has no network.

Evidence boundary

Earlier native Hyper-V testing reproduced a changed-DHCP binding defect and validated the recovery fix in its QA guest. The final refreshed package passed isolated checks; native acceptance of the exact refreshed disk still needs to be recorded. The reference panels above are not host screenshots.

Huawei Cloud 1 - request the right format



SCREENSHOT - Actual OTL customer request capture for the Huawei Cloud platform.

1. Choose Huawei Cloud x86, not FusionCompute. Obtain the Cloud QCOW2 ZIP and verify its hash.

2. Extract the supplied image and review the image service requirements for your region/product. This delivery is x86-64, not Kunpeng/ARM64.

3. Ask your cloud administrator to confirm supported Ubuntu guest settings, firmware, drivers, image size and networking before import.

> This is an OTL request screenshot, not a Huawei Cloud console screenshot. Native Huawei import and lifecycle acceptance remain pending. Do not equate Cloud Stack, public Cloud IMS and FusionCompute procedures.

Huawei Cloud 2 - image service to ECS

REFERENCE ILLUSTRATION - not a captured host screen

Huawei Cloud reference path	Your selection
Stage 1	Upload the verified image using the approved image-import process
Stage 2	Register a private system image in IMS
Stage 3	Select the correct x86 architecture/guest/firmware options
Stage 4	Create an ECS from that private image
Stage 5	Select VPC/subnet/security group and open its console
Stage 6	Confirm Linux boot, address and OTL HTTPS

1. Use the official region-specific image-import workflow. If OBS is required by that workflow, use an approved bucket with appropriate access controls and costs.

2. Register the system image with the correct OS, architecture and minimum disk size. Do not guess boot-mode conversion requirements.

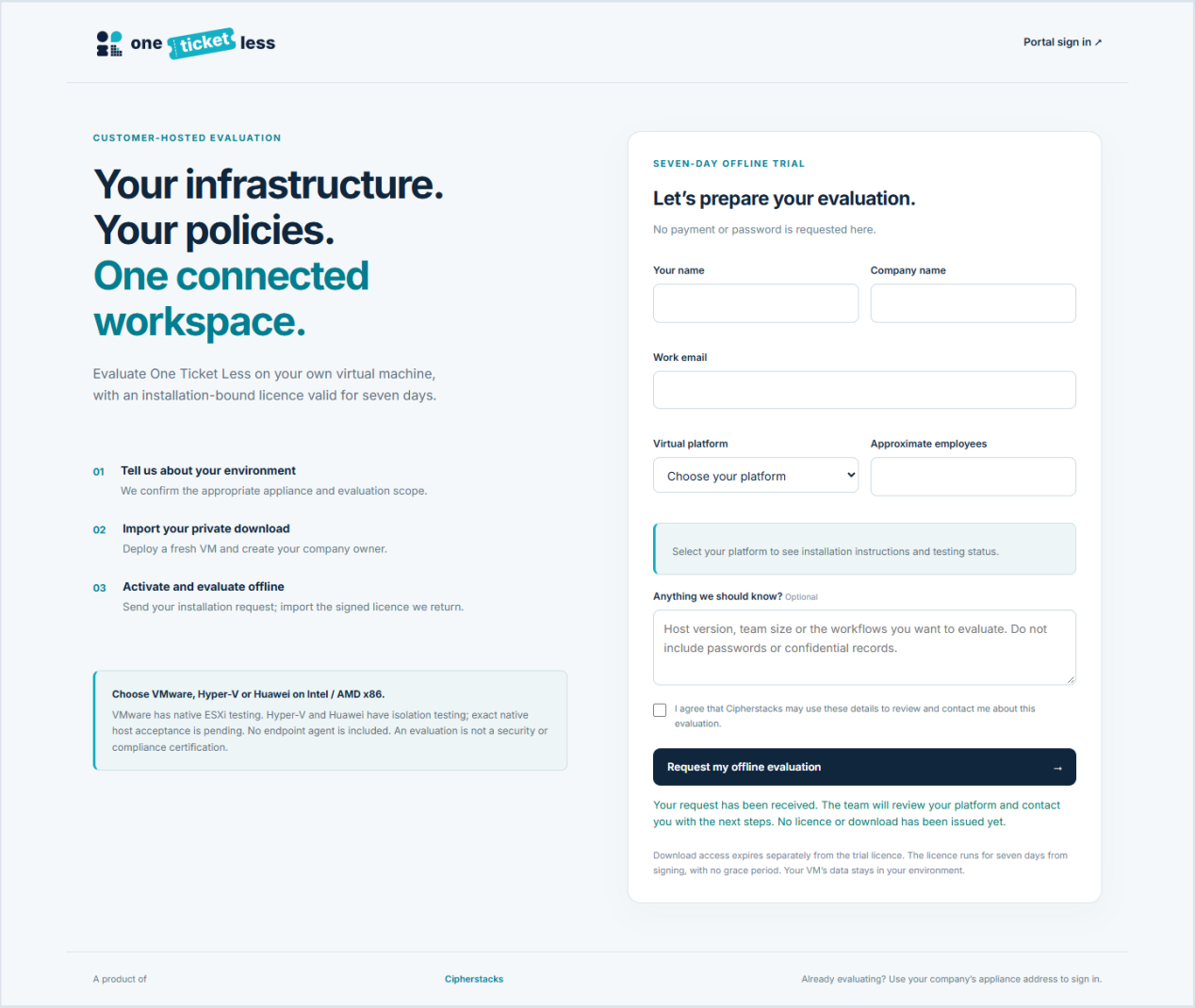
3. Create a test ECS from the private image. Choose workload sizing, approved storage, subnet and security rules.

4. Allow HTTPS from approved clients. Restrict management access; do not expose PostgreSQL or the application port.

5. Verify actual console boot and a reachable VM address. Only then complete the shared OTL setup chapters.

Reference: Huawei Cloud IMS image-file overview. Menu names and requirements vary by region; consult the documentation for the actual purchased service.

FusionCompute 1 - separate VHD package



SCREENSHOT - Actual OTL customer request for the FusionCompute package.

1. Select FusionCompute x86 and obtain its separately labelled VHD ZIP. Do not substitute a Cloud QCOW2, VMware OVA or Hyper-V VHDX package without a qualified conversion process.

2. Verify the hash, extract the delivery and give its instructions to the FusionCompute administrator.

3. Record the exact FusionCompute release and supported import/template requirements before attempting production deployment.

> No native FusionCompute environment was available for screenshots or validation. The delivered VHD passed isolated disk/controller/boot checks only. A vendor-specific template/descriptor or conversion may be needed by your host version; do not rename a VHD to pretend it is an OVA.

FusionCompute 2 - qualify and boot

REFERENCE ILLUSTRATION - not a captured host screen

FusionCompute reference checklist	Your selection
Host administrator	Confirm supported existing-disk/template import for this release
Guest architecture	x86-64
Disk package	FusionCompute VHD delivery
Virtual hardware	Host-qualified firmware, storage and NIC configuration
Placement	New VM, approved datastore and site network
Acceptance	Boot, DHCP/static network, HTTPS, restart and graceful shutdown

1. Follow the exact import steps from your qualified host instructions. If the host requires a different template, stop and request the supported packaging rather than improvising on customer data.

2. Create a fresh test VM and map its NIC to the approved site network. Review disk allocation and workload sizing.

3. Open its console, power on and wait for Linux/OTL first boot. Record any missing-driver or firmware errors.

4. Pass the same Linux, browser, activation and restore checklist used for other platforms. Treat this as a pilot until native acceptance is signed off.

Before moving on: A native-host acceptance record is available before a production claim is made. The remaining OTL browser steps are shared with VMware and Hyper-V.

Shared 1 - verify Linux startup

REFERENCE ILLUSTRATION - not a captured host screen

What you should see at first boot	Your selection
Console	Ubuntu login / OTL ready message
Portal URL	https://YOUR-VM-IP (not the hypervisor IP)
Services	database + app + https + worker
Initial load	Several minutes; do not interrupt images.tar import

```
ip -br -4 address
ip route
timedatectl status
df -h / /opt
sudo systemctl status otl-first-boot --no-pager
sudo journalctl -u otl-first-boot -n 80 --no-pager
```

1. Sign in with unique delivered console credentials and change the password when prompted.

2. Use the physical virtual NIC address, not a Docker bridge. Reserve DHCP or configure a static address from the console.

3. Check the first-boot service. It validates the bundle, loads packaged images and creates private database credentials.

4. If network configuration was wrong, correct it and restart otl-first-boot. Do not delete .env or secrets to retry.

Before moving on: The VM has the right address/time and can reach any required internal DNS/time services. Full Netplan and diagnostic commands are in the appendix.

Shared 2 - trusted HTTPS and setup key

```
cd /opt/oneticketless
sudo openssl x509 \
+  -in deployment/oneticketless-root-ca.crt \
+  -noout -fingerprint -sha256 -dates
sudo otl-show-setup-key
```

REFERENCE ILLUSTRATION - not a captured host screen

Keep these two files separate	Your selection
Public HTTPS root CA	deployment/oneticketless-root-ca.crt; verify fingerprint and trust
One-time owner setup key	Private setup-key file; only the authorised owner needs it
Never distribute	Private CA keys, database secrets or vendor signing keys

1. Open the VM URL from an approved workstation. Trust the verified appliance CA through your company process, or use an approved customer certificate.

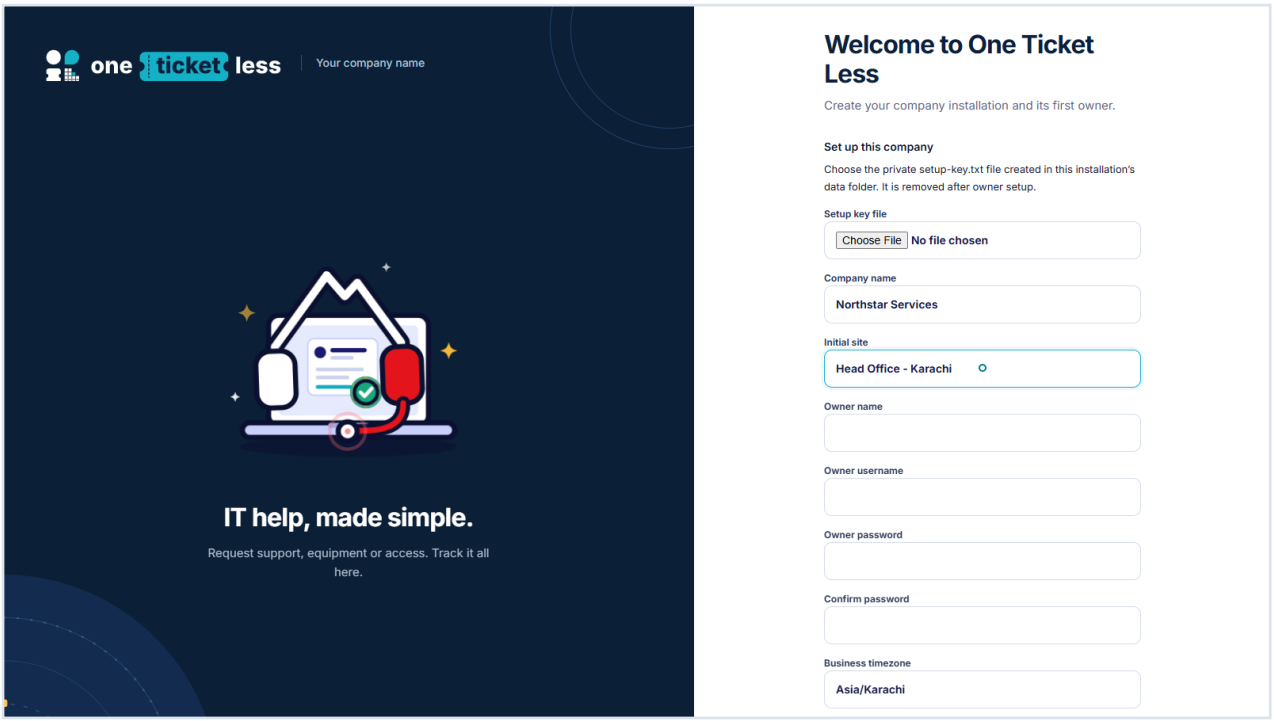
2. Verify the certificate fingerprint out of band. Do not make browser warning bypasses the permanent installation method.

3. At the authenticated VM console, retrieve the owner setup key. Transfer its private file securely if the browser form needs a file.

4. Protect setup-key copies and remove temporary copies after successful owner creation. Never include the key in a screenshot or tutorial.

Before moving on: The workstation trusts the correct HTTPS endpoint, and the owner has the private setup-key file. No live key is printed in this handbook.

Shared 3 - create company and owner



SCREENSHOT - Actual earlier OTL first-run form with fictional training details.

1. Select the private setup-key file. Enter company name and initial site.

2. Enter the owner name and unique username. Choose a private password and confirm it.

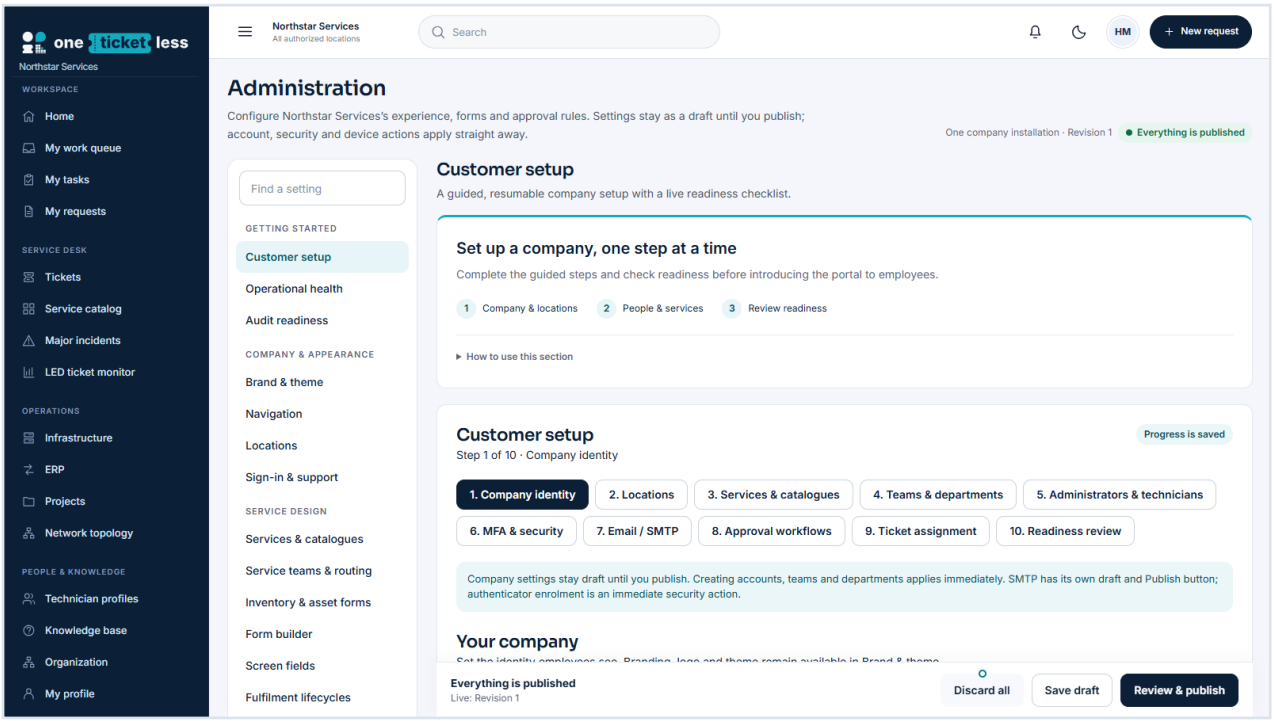
3. Choose the business timezone. The owner is your organisation's administrator, not a vendor user.

4. Submit once and wait for the workspace. Keep the VM identity; reinstalling after creating the installation request can make the returned licence invalid.

Before moving on: The owner can sign in. Unlicensed normal writes remain blocked until activation; this is expected.

CUSTOMER DEPLOYMENT GUIDE / 18

Shared 4 - find Licensing



SCREENSHOT - Actual training workspace after first-run owner setup.

1. Open One Ticket Less administration and find Licensing using its navigation or settings search.

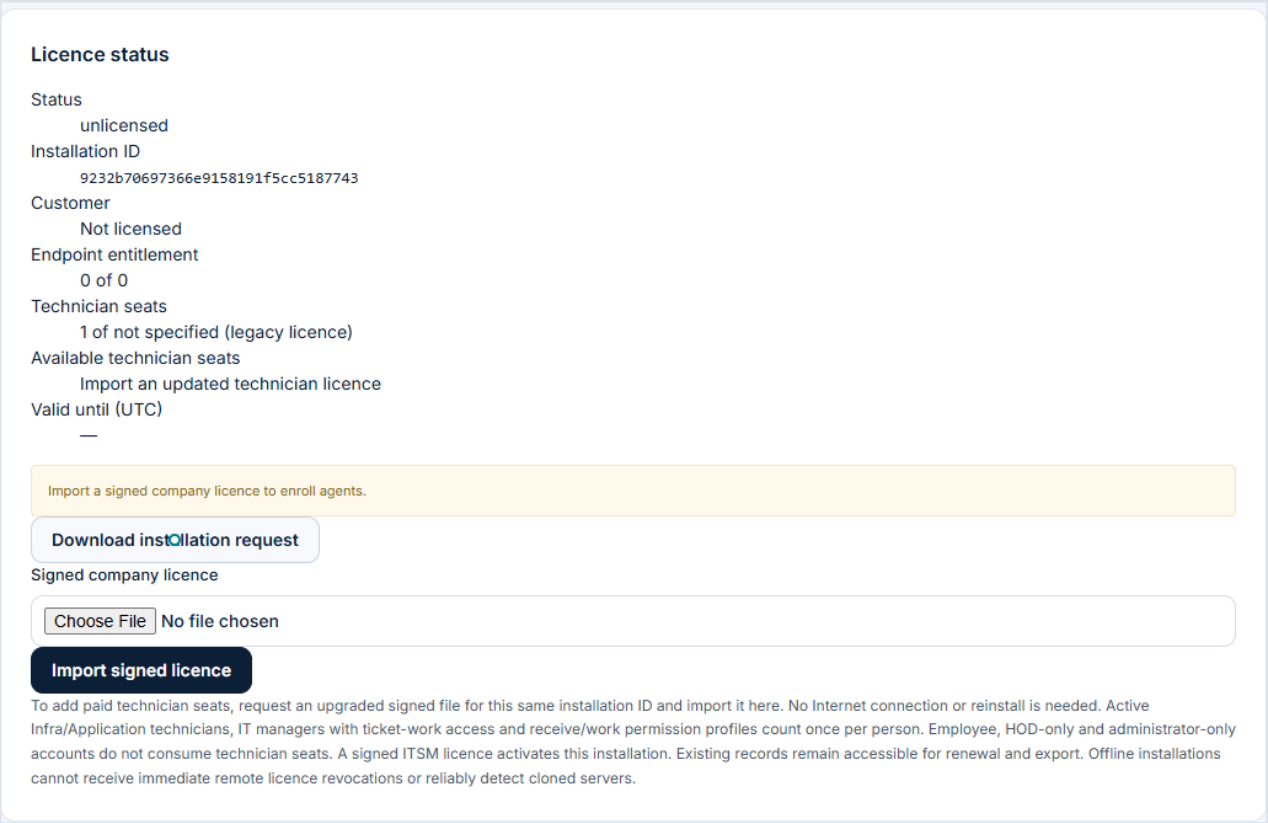
2. Do not confuse brand settings, maintenance signing or account passwords with installation licensing.

3. Check installation status before importing anything. New installations normally show unlicensed.

4. If there is already an active company identity, confirm that this is the correct VM rather than resetting setup.

> **Before moving on:** You are signed in directly as the authorised company administrator, on the intended customer installation.

Shared 5 - download installation request



SCREENSHOT - Actual licensing controls from the earlier training release; no private signing key is present.

1. Choose Download installation request and save the JSON unchanged.

2. Send it through the approved channel with company name, desired 30-day term and technician allowance.

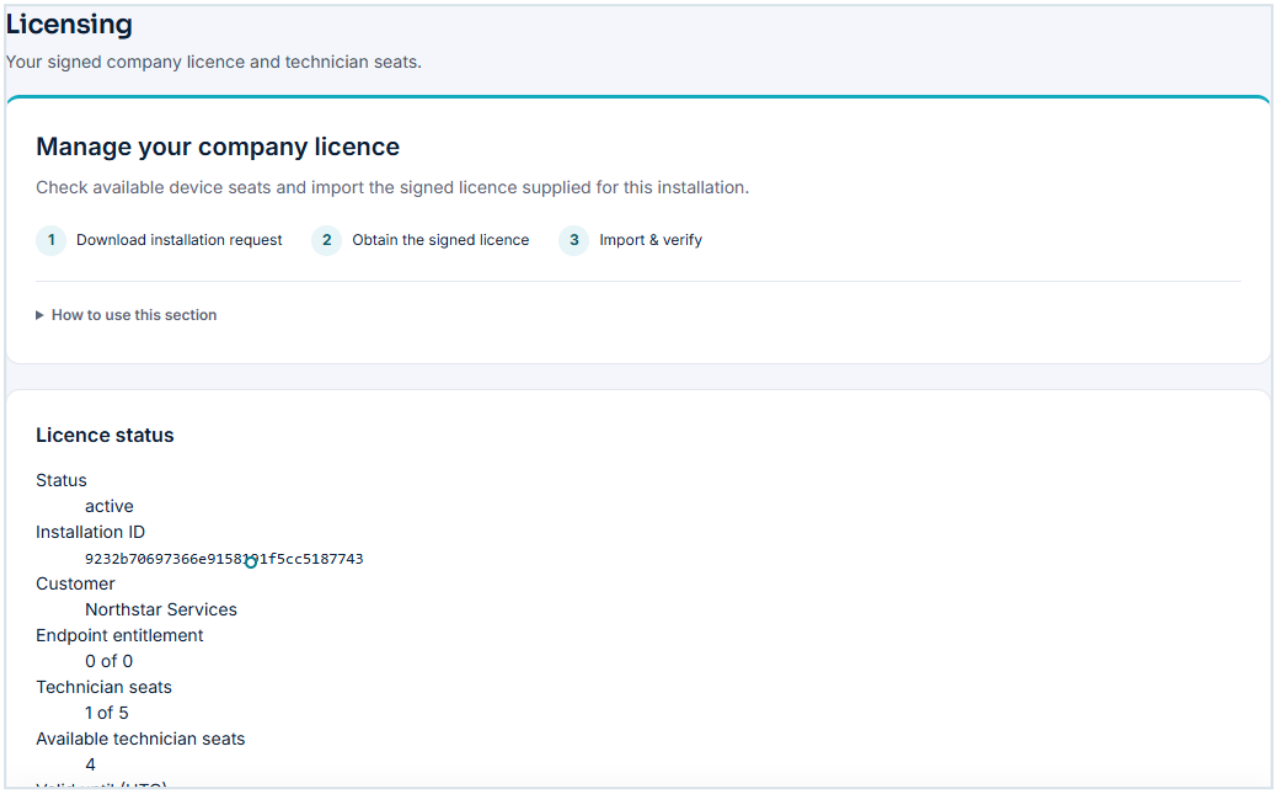
3. Use a separate connected computer/media process if the appliance is fully offline. The appliance itself does not need internet.

4. Wait for the signed licence. Do not edit quotas, dates, customer or installation ID in either JSON file.

Some legacy training wording mentions agents. This customer appliance includes no endpoint agents. Your issued licence must contain the intended ITSM entitlement and technician allowance.

Before moving on: The vendor has the request from this exact installation and the agreed commercial term.

Shared 6 - import and verify activation



SCREENSHOT - Actual earlier training activation with five technician seats. The screenshot is not a 30-day entitlement.

1. Select the returned signed company licence in Licensing and import it.

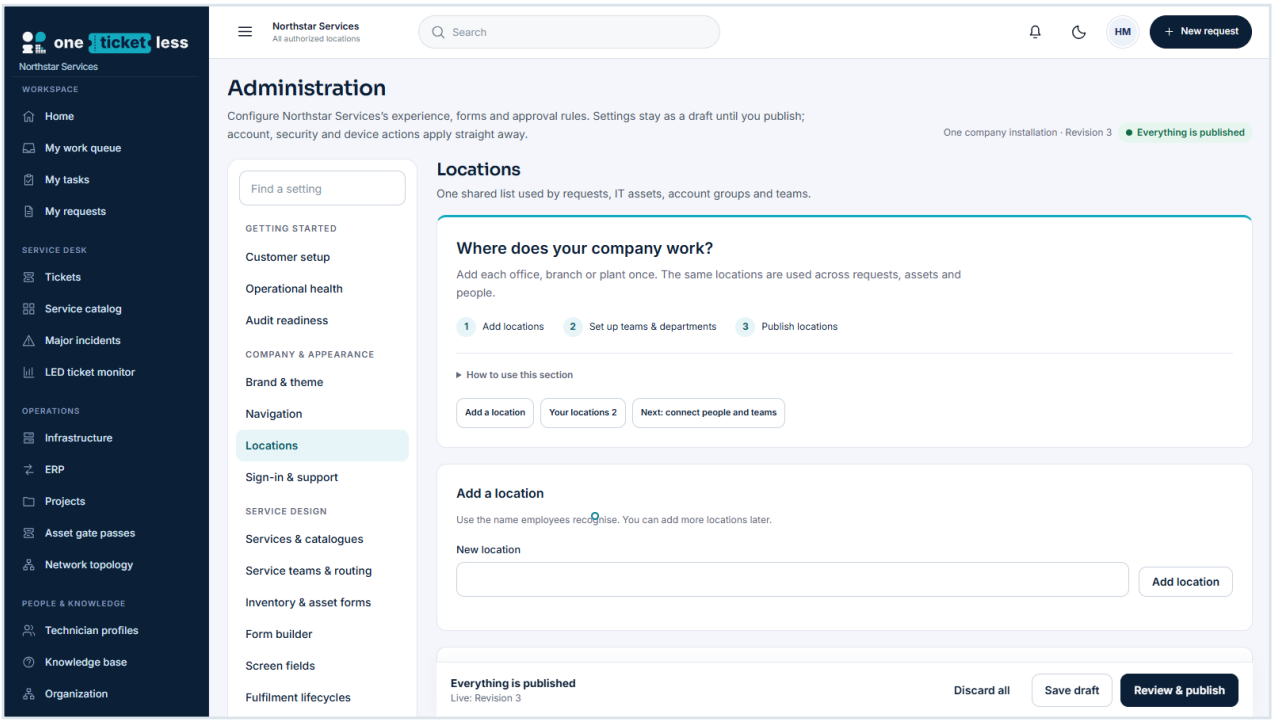
2. Confirm Status active, correct company/installation, expiry date and technician quota. Scroll within the page to inspect fields not visible in the screenshot.

3. For your one-month arrangement, confirm the actual issued dates. Do not infer the term from the screenshot or the file name.

4. Create an authorised test task/request and sign out/in once. Save the licence and installation record securely.

Before moving on: Normal writes work only with a valid applicable licence. Modified, wrong-installation or older incompatible terms should not be accepted.

Shared 7 - locations, users and workflow



SCREENSHOT - Actual Locations settings from the training company.

1. Create all real sites before assigning people and inventory. Use the company's naming convention.

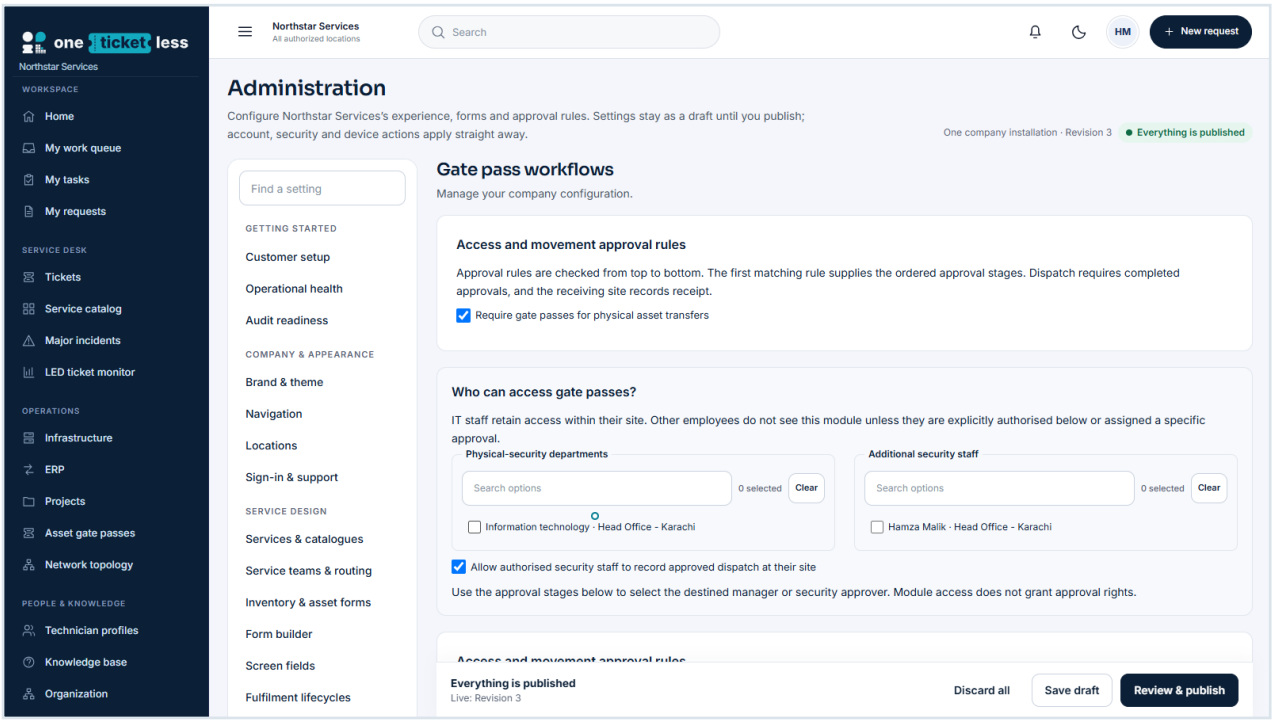
2. Create/import departments and employees, then assign HOD/manager/technician roles and team memberships.

3. Create service types and catalogues, request fields and approval rules. Configure the desired manual/round-robin routing.

4. Save/review/publish configuration where applicable. Then test using non-admin users at different sites.

> **Before moving on:** An employee's actual request follows the same route shown in its preview. HOD exceptions and approval-free policies are tested separately.

Shared 8 - sign-in, mail and gate passes



SCREENSHOT - Actual configurable gate-pass workflow page from the training release.

1. Set gate-pass request/approval access to IT and authorised security staff. Confirm the company logo appears in print preview.

2. Configure internal SMTP and test a password-reset email. The reset-link hostname must resolve from the client network.

3. Configure MFA according to the customer policy. Do not copy the demo company's bypass policy into a real company.

4. Test assets, custody, conversation, gate-pass approval and printed output with the intended roles.

> **Before moving on:** Mail/recovery, role visibility, approval routing and printed company identity all work before handover.

Finish - backup, reboot and acceptance

REFERENCE ILLUSTRATION - not a captured host screen

Customer handover evidence	Your selection
Infrastructure	Native host import/boot/network/shutdown/restart result
Security	Trusted HTTPS; unique passwords; policy and known findings recorded
Licence	Customer, installation, quota and exact validity confirmed
Workflow	Employee -> HOD/manager -> technician -> completion verified
Recovery	Database + keys + files + TLS/config backup; populated restore rehearsed
Ownership	Named maintenance owner, renewal contact and backup retention

1. Take a coordinated backup and copy it encrypted off the VM. Include server keys and TLS/configuration, not just a database dump.

2. Reboot in an approved window. Confirm the address/HTTPS, sign-in, licence and services recover.

3. Restore to a separate recovery VM and verify populated records, attachments and audit history.

4. Document unresolved platform/security conditions and customer acceptance. Never market a labelled reference illustration as a native test result.

Continue into the command appendix

The following 16 sections contain the complete Linux operations guide: static networking, CA trust, private setup key handling, licence renewal, diagnostics, coordinated backup commands, maintenance and troubleshooting. Commands run inside the OTL VM unless explicitly marked otherwise.

CUSTOMER DEPLOYMENT GUIDE / 01

Before you begin

This guide installs the supplied OTL virtual appliance. The appliance is a headless Ubuntu Linux server with the application, PostgreSQL database and HTTPS proxy already packaged. You use a browser on another computer; a Linux desktop is not needed.

Choose the right installation method

Recommended: import the vendor-supplied VM on a compatible virtualisation host. Run the Linux commands in this guide **inside that OTL VM**, unless a block explicitly says Windows/Hyper-V host or client workstation.

An existing bare-metal Linux server needs a virtualisation layer capable of importing the disk, or a separately supplied and qualified OTL container bundle. Do not run the appliance commands on an unrelated server or install Docker/application source manually from this guide. A VMDK is a virtual disk, not an ISO installer.

Have these items ready

1. The correct release archive, authenticated download access and its SHA-256 value from the vendor.

2. A supported x86-64 host, administrative access, VM storage, a switch/port group and the correct VLAN.

3. A reserved VM IPv4 address, gateway, DNS and an internal time source. Record who owns DNS and certificates.

4. Unique delivery console credentials, a new company-owner password and an approved backup destination.

5. The agreed licence term and technician allowance. A 30-day licence must be issued explicitly; the seven-day evaluation is a different term.

Sizing and network policy

The reference build uses 4 vCPUs, 8 GB RAM and a 64 GB logical system disk. These are starting configuration values, not a capacity guarantee. Agree sizing based on employees, concurrent users, attachments and retention. Allow storage for the VM, backups and restore testing; thin disks still grow.

> Initial access needs HTTPS TCP 443 from approved client networks. HTTP TCP 80 is mapped by the proxy and normally redirects to HTTPS. Do not publish PostgreSQL 5432 or application 3000. SSH, if enabled, should be restricted to an approved management network. Offline operation does not need public internet; internal DNS, time, mail and directory services may still be used.

CUSTOMER DEPLOYMENT GUIDE / 02

Pick and verify your download

Request the platform-specific download from One Ticket Less. Download on an approved connected machine and transfer through your organisation's approved offline-media process. Keep the release notes, testing status and integrity value with the package.

VMware / ESXi

Use the .ova package. It contains the OVF definition and VMDK. Deploy the OVA as a new VM; do not attach a live customer disk to another company.

Microsoft Hyper-V

Use the Hyper-V ZIP containing a .vhdx and its instructions/helper. Create a Generation 2 VM. If Secure Boot is enabled, use the Microsoft UEFI Certificate Authority template for Linux.

Huawei Cloud x86 / FusionCompute x86

Cloud uses the QCOW2 package; FusionCompute uses the separately labelled VHD package. Use the exact platform-specific import instructions. These are x86-64 images, not Kunpeng/ARM images.

Verify the downloaded archive - Linux workstation

```
sha256sum /path/to/OneTicketLess-release.ova
# Compare the full value with the authenticated vendor checksum.
```

Or verify on a Windows workstation - PowerShell

```
Get-FileHash -Algorithm SHA256 -LiteralPath `
  "C:\Downloads\OneTicketLess-release.ova"
```

Replace the example filename with your actual archive. Compare every character of the hash. If it differs, stop and obtain a fresh package; do not edit the manifest to make it pass.

> **Testing status:** all four current formats passed isolated boot/controller/network recovery tests. Earlier native VMware and Hyper-V checks exist, but the exact final refresh still needs native acceptance on the target host. Huawei native validation remains pending. Read the delivered TESTING-STATUS/KERNEL-STATUS information; isolated tests are not universal host certification.

CUSTOMER DEPLOYMENT GUIDE / 03

Import and start the virtual machine

VMware / ESXi - host web interface

1. Sign in to the host/vCenter using your approved administrator account. Select deployment from an OVF/OVA file.

2. Choose the verified OVA, a new VM name, datastore and compute placement. Review the hardware definition before confirming.

3. Map its network to your actual port group/VLAN. Ensure the virtual NIC is connected at power-on. Use the firmware/controller settings delivered in the OVF.

4. Review CPU, RAM and disk allocation, finish import, then open the VM console and power on. Do not interrupt the first image load.

Hyper-V - Windows host

Extract the ZIP and keep an untouched copy of the delivery disk. The supplied Create-HyperV.ps1 copies the VHDX into a new VM directory and does not start the VM. Run an elevated PowerShell window on the **Hyper-V host**.

```
Get-VMSwitch
.\Create-HyperV.ps1 `
  -VhdxPath "D:\OTL-Download\oneticketless.vhdx" `
  -StorageRoot "D:\VirtualMachines" `
  -SwitchName "Company-LAN" `
  -VMName "OneTicketLess" -EnableSecureBoot -WhatIf
```

Review the proposed action, repeat without -WhatIf, then start the new VM in Hyper-V Manager. Replace paths and switch name. The helper refuses existing VM names/folders. Without the helper, create Generation 2, attach a copy of the VHDX to SCSI, select the correct switch and review the Linux Secure Boot CA template.

Huawei - host-specific import

Use your Huawei administrator's image import process with the correct Cloud QCOW2 or FusionCompute VHD, then attach network/storage and boot a test VM. Storage controller, image service conversion and firmware requirements vary by product/version. Obtain native-host acceptance before business use; this guide does not invent one universal Huawei command.

CUSTOMER DEPLOYMENT GUIDE / 04

First boot and Linux health checks

Open the **OTL VM console**, not the hypervisor terminal. Sign in using the unique delivery console credentials and change the password if prompted. These credentials are separate from the browser company-owner account.

Confirm the VM address and time

```
hostnamectl
ip -br -4 address
ip route
timedatectl status
df -h / /opt
free -h
```

Use the IPv4 address on the physical virtual NIC (such as ens160 or eth0), not a Docker bridge address. The example used throughout this guide is **192.0.2.50**; it is a documentation address and must be replaced with your real internal address. The ESXi/Hyper-V management address is not the OTL address.

Inspect startup without exposing secrets

```
sudo systemctl status docker --no-pager
sudo systemctl status otl-first-boot --no-pager
sudo journalctl -u otl-first-boot -n 80 --no-pager
cd /opt/oneticketless
sudo docker compose --env-file deployment/.env \
  -f deployment/compose.postgres.yaml ps
```

Expected services: database, app, worker and https. The worker does not have a Docker health probe; running is expected. Other services should settle to healthy. First boot verifies the bundle, loads offline images, generates database secrets and starts the services. Allow several minutes on slower storage.

If startup failed after correcting networking

```
sudo systemctl restart otl-first-boot
sudo journalctl -u otl-first-boot -n 80 --no-pager
```

> Do not delete deployment/.env, appliance-secrets, customer volumes or installation identity files to retry setup. Do not rerun image finalisation. These actions can lose data or break licence binding. Never use docker compose down -v or docker system prune as troubleshooting shortcuts.

CUSTOMER DEPLOYMENT GUIDE / 05

Use a stable network address

A DHCP reservation is the simplest option: reserve the appliance NIC's MAC address in your DHCP service. Confirm the correct VLAN, gateway and DNS. A stable address avoids broken bookmarks and certificate/name mismatches.

Optional static IPv4 - Linux VM console only

Inspect the existing Netplan files first. Adapt the active interface stanza; do not leave conflicting definitions for the same NIC. Keep the VM console open because network changes can disconnect SSH. Back up the current directory before editing.

```
ip -br link
sudo ls -l /etc/netplan
sudo cp -a /etc/netplan /root/netplan-before-otl
sudoedit /etc/netplan/YOUR-ACTIVE-FILE.yaml
```

Example content below is a **template**. Replace interface, address/prefix, gateway and DNS with values supplied by your network administrator. Preserve other required interfaces and settings.

```
network:
  version: 2
  ethernets:
    ens160:
      dhcp4: false
      addresses: [192.0.2.50/24]
      routes:
        - to: default
          via: 192.0.2.1
      nameservers:
        addresses: [192.0.2.53]

sudo netplan generate
sudo netplan try --timeout 120
# Confirm only when connectivity is correct.
ip -br -4 address
ip route
```

If cloud-init manages the network, coordinate its configuration with your Linux administrator; an edit may otherwise be overwritten. Do not disable provisioning blindly. In the current release, restarting otl-first-boot can refresh an unchanged generated IP/internal-TLS binding when exactly one replacement NIC address exists. It deliberately preserves custom domains and proxy configurations.

CUSTOMER DEPLOYMENT GUIDE / 06

Open the portal and trust HTTPS

1. Read the portal URL displayed by the VM console. From a workstation on an allowed network, open https://YOUR-VM-IP.

2. Initial HTTPS uses an appliance-generated private certificate authority. Have your IT security team verify and distribute its public root certificate through an approved trust process.

3. After trusting the correct CA, reopen the URL. A hostname/IP mismatch still requires correcting the address/certificate; CA trust alone cannot fix it.

Locate the public root CA - Linux VM

```
cd /opt/oneticketless
sudo ls -l deployment/oneticketless-root-ca.crt
sudo openssl x509 \
  -in deployment/oneticketless-root-ca.crt \
  -noout -subject -issuer -dates -fingerprint -sha256
```

The first-boot service exports this **public certificate**. Transfer it over an authenticated channel or controlled media and verify its SHA-256 fingerprint out of band. Never transfer Caddy's private CA key or server private keys to user workstations.

Trust on an approved Ubuntu/Debian client workstation

```
# Run on the CLIENT, using the verified public certificate.
sudo install -m 644 oneticketless-root-ca.crt \
  /usr/local/share/ca-certificates/oneticketless-root-ca.crt
sudo update-ca-certificates
```

For Windows clients, IT should distribute the verified public CA through the organisation's certificate policy/Trusted Root Certification Authorities store. Some browsers maintain separate trust settings; follow company policy.

Health check using the explicit CA - Linux VM

```
cd /opt/oneticketless
curl --cacert deployment/oneticketless-root-ca.crt \
  https://YOUR-VM-IP/health
```

> Do not make permanent browser certificate bypasses or curl -k part of customer acceptance. A public certificate requires the appropriate DNS/reachability; an offline company may instead use its own internal CA. HTTP access is not a substitute for trusted HTTPS.

CUSTOMER DEPLOYMENT GUIDE / 07

Create your company and first owner

Retrieve the one-time setup key - authenticated VM console

```
sudo otl-show-setup-key
```

This prints sensitive setup material. Read it privately, do not record it in a tutorial or support log, and do not send it to other employees. Initial owner setup accepts the private setup-key file created by the installation. If the browser needs a file, create a protected copy as follows.

```
sudo sh -c 'umask 077; otl-show-setup-key > /root/otl-setup-key.txt'
```

Transfer that file to the authorised setup workstation through a secure, approved process. Do not weaken /root permissions. Delete the transferred temporary copy after successful setup according to your security policy. The original one-time setup key is consumed by owner creation.

Complete the first-run browser form

1. Open the portal URL and select the setup-key file.

2. Enter your real company name and initial site. Use the customer name agreed for licensing.

3. Enter the owner's name and unique username. This is a customer administrator, not a vendor-console account.

4. Choose and confirm a strong private owner password. Select the business timezone carefully and submit once.

5. Wait for the successful navigation into the workspace. If an error appears, preserve its wording and check service health rather than repeatedly creating owners.

A newly created owner can reach activation-related settings, but a fresh unlicensed offline appliance must not permit normal operational writes. If licensing is required, this is expected and is not a broken installation.

> No universal customer admin password is supplied in this guide. Do not reuse demo passwords, vendor passwords or the Linux console password for the owner. If first-run setup is no longer offered, verify whether this VM has already been initialised; do not reset the database.

CUSTOMER DEPLOYMENT GUIDE / 08

Activate 30 days of offline access

The licence is signed by One Ticket Less and bound to the installation identity. Your server does not need to contact a licensing website. A separate approved device can carry the request and returned licence between your offline network and the vendor.

1. Sign in directly as the company owner and open **One Ticket Less administration > Licensing**.

2. Download the installation request JSON. Keep the VM intact after generating it; do not reinstall or create a new identity.

3. Send that request to your authorised One Ticket Less contact. Confirm company name, **30-day term**, start/end dates, business timezone and the purchased technician allowance.

4. The vendor issues a signed licence for that request. A seven-day website trial does not automatically become one month; the vendor must issue the agreed 30-day validity.

5. Transfer the returned licence JSON into the offline environment and import it from Licensing. Do not edit its contents.

6. Confirm active status, installation/customer match, expiry date and technician limit. Save the licence and agreement in your protected deployment records.

7. Create a small test task/request to confirm operational writes are enabled. Log out and sign back in once to validate normal access.

Renewal or additional technicians

Contact the vendor before expiry. For a quota increase, request a newer signed licence for the **same installation** with the new allowance. Import it in Licensing; no reinstall is required. Older, modified or wrong-installation licences should be rejected. Disabling an eligible technician can free a seat; regular employees and admin-only accounts do not all count as technicians.

What happens at expiry?

When the applicable validity/grace policy no longer permits access, operational writes and automation are blocked. Records remain available for permitted reading/export and renewal. Expiry is not a data-deletion mechanism. Confirm the exact expiry and any grace terms shown by your issued licence.

> Keep the VM clock accurate using an approved internal time source. Do not alter it to extend access. Fully offline software cannot offer absolute resistance to an administrator restoring a complete VM snapshot and its clock state; the signed licence does not remove that limitation.

CUSTOMER DEPLOYMENT GUIDE / 09

Configure OTL for your company

Use the company administration GUI after activation. Most configuration changes use draft, review and publish; some security/device actions apply immediately. Read the action's on-screen effect before confirming.

1. Brand & theme: enter company details, upload a transparent PNG logo and verify it in the sidebar and gate-pass print preview.

2. Locations: create every required site/location before importing employees and assets. Decide who can see each site.

3. Services & catalogues: add Infrastructure, Application/SAP and your own service types. Define request categories and the fields people must fill.

4. Accounts, roles and directory: create/import employees, departments, HODs, IT managers and technicians. If LDAP/AD is used, configure and test it with your directory administrator; offline directory access stays within your network.

5. Teams and routing: define network, systems, security and application teams, skills, availability and assignment method. Test manual and automatic routing.

6. Approval workflows: define additional/replacement/upgrade routes, HOD/C-level exceptions and gate-pass authorities. Compare the preview with an actual test request.

7. Inventory: configure asset types and relevant fields, locations, custody, renewal dates and technician permissions. Import real customer data only after checking a small sample.

8. Security and communication: configure MFA policy, password reset, SMTP, gate-pass access and audit review. Use company policy rather than demo settings.

Offline mail, directory and password reset

SMTP/LDAP/AD can use internal servers if routing and certificates allow. Email reset links need a portal URL recipients can resolve and reach. DNS A/CNAME records route a hostname; they do not themselves send email. Test a reset link end to end with a non-admin account. Without an accessible mail service, establish an administrator-assisted recovery procedure.

> Do not expose the vendor signing key to the customer appliance. The customer holds public verification keys and its signed licence. No endpoint-agent installation is part of this deployment.

CUSTOMER DEPLOYMENT GUIDE / 10

Daily Linux operations

These commands run inside the OTL VM. They inspect state or restart only the stated OTL component. Use a maintenance window for actions that interrupt users.

A convenient shell function

```
cd /opt/oneticketless
otl() {
  sudo docker compose --env-file deployment/.env \
    -f deployment/compose.postgres.yaml "$@"
}
otl ps
```

The function exists only in the current shell. Define it again in a new terminal. It uses the shipped deployment file and existing secrets.

Logs and database readiness

```
otl logs --tail=80 app
otl logs --tail=80 worker
otl logs --tail=80 https
otl exec -T database pg_isready -U postgres -d postgres
sudo journalctl -u otl-first-boot -n 80 --no-pager
```

Controlled restart

```
# Briefly interrupts app sessions; choose a quiet window.
otl restart app worker
otl ps
# Full guest restart, only during an approved maintenance window:
sudo systemctl reboot
```

After reboot, verify portal HTTPS, sign-in and the worker. For a planned guest shutdown, use sudo systemctl poweroff and allow it to stop before manipulating disks on the host.

Storage and time

```
df -h / /opt
sudo docker system df
timedatectl status
sudo ss -lntp
```

Watch disk growth, failed backups, abnormal container restarts and time drift. Avoid printing full environment/configuration files into support tickets: they can contain secrets. Review and redact logs before sharing them.

CUSTOMER DEPLOYMENT GUIDE / 11

Back up database, keys and files

A usable backup needs the PostgreSQL database **and** matching customer files/encryption keys, deployment configuration and TLS state. Keep an encrypted off-VM copy. A snapshot alone is not a tested recovery strategy.

Application database backup - Linux VM

With the otl shell function from section 10 defined, create a unique backup file through the shipped verifier. The command prints the destination and result; it does not copy the backup off the VM.

```
stamp=$(date -u +%Y%m%dT%H%M%SZ)
otl exec -T app node scripts/backup.mjs \
  "/app/data/backups/otl-${stamp}.dump"
```

The database backup includes database-stored attachments. Server encryption keys and any filesystem data are separate. Check the success output and retain the exact timestamp. An existing destination is refused.

Capture a consistent full set - maintenance window

The next page provides a root-shell example to pause writes and capture both data and configuration. It restarts app/worker on exit, including a failed command. Adjust the approved backup destination; ensure enough free space first. Archives include secrets and require encryption and restricted access.

Restore procedure - controlled recovery VM

1. Prepare a separate recovery VM with the matching approved release. Keep production intact and avoid simultaneous network/identity conflicts.

2. Restore the database into a new empty PostgreSQL destination, using scripts/restore-postgres.mjs with DESTINATION_DATABASE_URL supplied securely. The tool refuses populated destinations, checks the audit chain and clears restored sessions.

3. Restore the matching customer-files volume, deployment secrets/configuration and TLS state before starting OTL. Do not generate replacement encryption keys.

4. Verify company identity, signed licence, users, ticket/asset counts, sample attachments, approvals, HTTPS and a test write. Record the result.

5. Only then perform an agreed cutover. Licence binding and snapshot age must be reviewed with support; never finalise/reset an existing customer image.

> The automated release restore test used a fresh one-user fixture and two data/key files. Each customer still needs a populated-data restore rehearsal. Do not treat a successful dump command as proof of disaster recovery.

CUSTOMER DEPLOYMENT GUIDE / 12

Full backup command example

Run inside the appliance, in an approved maintenance window. This captures a raw PostgreSQL custom dump plus private files and proxy state without deleting any volume. The raw dump is not the application audit-verifying restore tool. Validate the archive contents and rehearse recovery separately.

```
sudo -i
cd /opt/oneticketless
set -eu
umask 077
backup="/root/otl-backups/$(date -u +%Y%m%dT%H%M%SZ)"
mkdir -p "$backup"
otl() {
  docker compose --env-file deployment/.env \
    -f deployment/compose.postgres.yaml "$@"
}
# Resume application services even if a capture fails.
trap 'otl start app worker >/dev/null' EXIT
otl stop app worker
otl exec -T database pg_dump -U postgres -d otl \
  -Fc --no-owner --no-acl > "$backup/database.dump"
# One-off app container can read its existing customer volume.
otl run --rm --no-deps -T --entrypoint tar app \
  -C /app/data -cf - . > "$backup/customer-files.tar"
# Capture private proxy CA and certificate state as well.
otl exec -T https tar -C /data -cf - . \
  > "$backup/https-data.tar"
otl exec -T https tar -C /config -cf - . \
  > "$backup/https-config.tar"
tar -C /opt/oneticketless -cf "$backup/deployment.tar" \
  deployment
otl exec -T database pg_restore --list \
  < "$backup/database.dump" > "$backup/database-contents.txt"
(cd "$backup" && sha256sum *.dump *.tar > SHA256SUMS)
otl start app worker
trap - EXIT
otl ps
printf 'Backup set: %s\n' "$backup"
exit
```

Keep the entire timestamped directory together. Encrypt it before transfer to an approved backup system, retain its key separately, and confirm the off-VM copy can be read. The customer-files archive may include earlier backups; plan retention to avoid uncontrolled growth. A trusted administrator should adapt this example to the company backup service and storage design.

CUSTOMER DEPLOYMENT GUIDE / 13

Updates and planned maintenance

The appliance has two maintenance layers: the Ubuntu operating system and the packaged OTL application/database/proxy. Do not mix an OS package update with an unreviewed container or database-major-version upgrade.

Inspect Ubuntu updates - requires an approved repository

```
uname -r
sudo apt update
apt list --upgradable
test ! -f /var/run/reboot-required || \
  cat /var/run/reboot-required
```

apt update refreshes repository metadata; it does not install upgrades. On a fully disconnected network it needs an approved internal mirror or an offline update process provided by your Linux/security team. It cannot fetch internet packages without connectivity.

Apply only an approved maintenance plan

Use the OTL maintenance workflow to record the release, preflight, current backup, independent approval, maintenance window and postchecks. Follow vendor instructions for the actual signed update payload. An offline licence renewal is not an application update and uses a separate signature purpose.

For OS security packages, the Linux administrator should review the proposed package transaction, take/rehearse backups and arrange a restart if needed. Avoid blind apt full-upgrade, distribution upgrades or a mainline kernel swap on a customer appliance. Do not run docker compose pull/build to obtain unreviewed images.

After an approved reboot

```
uname -r
sudo systemctl status otl-first-boot --no-pager
cd /opt/oneticketless
sudo docker compose --env-file deployment/.env \
  -f deployment/compose.postgres.yaml ps
```

Then check trusted HTTPS, local sign-in, an authorised test write, licence status, worker actions and a new backup. A newly installed kernel is not active until booted, unless a specific supported livepatch says otherwise.

> **Release limitation:** the 9 November 2026 appliance review still had pending/needed Ubuntu kernel advisories, with no newer supported repository candidate then available. Mitigations do not equal patches. Review the delivered kernel status and subsequent vendor updates before production use. Fully offline operation is not immunity to local or network attacks.

CUSTOMER DEPLOYMENT GUIDE / 14

Troubleshooting by symptom

No address / cannot open portal

Confirm NIC connected, correct switch/VLAN, DHCP lease or static configuration. Use the VM IP rather than the hypervisor IP. If client routing/firewall is blocked, fix that path first.

```
ip -br -4 address
ip route
sudo journalctl -u otl-first-boot -n 80 --no-pager
```

Unhealthy / first boot seems slow

Allow image load and startup to finish. Check free disk/RAM and the specific service logs. A service remaining unhealthy is not solved by disabling its healthcheck.

```
df -h
free -h
sudo systemctl status otl-first-boot --no-pager
```

Certificate warning

Verify CA fingerprint, client trust store, certificate validity, time and exact URL. Do not bypass checks permanently.

```
timedatectl status
```

Licence import refused / writes blocked

Check the signed file is for this installation, current term and trusted issuer. Check time and technician allowance. Do not edit the licence JSON; request a corrected/newer signed licence from the vendor.

Password reset mail missing

Check internal SMTP routing, authentication, certificate trust, mail logs and spam policy. Ensure the reset-link hostname resolves on the user network. A/CNAME records do not configure SMTP.

Setup says configuration exists

Existing .env/secrets are protected against regeneration. Use the existing installation. Do not delete configuration or initialise a new database to work around this message.

CUSTOMER DEPLOYMENT GUIDE / 15

Acceptance and handover checklist

Complete this checklist with the customer before distributing normal employee access. Record evidence and exceptions; an isolated test is not a substitute for the customer's native-host test.

[ ] Correct platform package and authenticated SHA-256 verified.

[ ] Target host version, firmware, storage controller and switch/VLAN recorded.

[ ] Unique console password changed; owner account and recovery contact recorded securely.

[ ] Stable IP/DNS, accurate internal time and trusted HTTPS verified from client devices.

[ ] Cold start, graceful shutdown and restart passed on the actual host.

[ ] Signed licence active; customer/installation, 30-day dates and technician quota checked.

[ ] Employee, HOD, technician and administrator permissions tested separately.

[ ] A real additional/replacement/upgrade approval preview matches the actual route.

[ ] Ticket assignment, communication, asset custody and gate-pass approval/print tested.

[ ] SMTP/reset link and directory integration tested where enabled; MFA policy agreed.

[ ] Database, customer encryption keys and TLS/configuration backed up off the VM.

[ ] A populated-data restore on a separate recovery VM passed and was documented.

[ ] Known kernel findings and native-platform limitations reviewed and accepted.

[ ] Maintenance owner, renewal date, backup retention and escalation contacts assigned.

Information to send support

Release filename/hash, host/version, VM sizing, time of issue, redacted error text, service status and relevant redacted logs. Include the installation request only through an approved licence-support channel. Never send passwords, private CA keys, vendor signing passphrases or unredacted deployment secrets.

Customer: _____
Platform/version: _____
Installer and date: _____
Customer acceptance / exceptions: _____

CUSTOMER DEPLOYMENT GUIDE / 16

Quick reference and document scope

Where things live

/opt/oneticketless
OTL packaged deployment root.

deployment/.env
Portal binding and deployment settings; protect it.

deployment/appliance-secrets
Database credentials; do not regenerate on an existing VM.

customer-files volume
Customer files and encryption keys; back up with the database.

postgres-data volume
PostgreSQL data; use coordinated logical backup/recovery.

https-data / https-config volumes
Proxy certificate/CA state and configuration state.

sudo otl-show-setup-key
Private one-time owner setup, authenticated VM console only.

Administration > Licensing
Installation request, signed licence import and validity/quota review.

Commands to avoid during routine support

Do not remove Docker volumes, run image finalisation, delete secrets, reset the installation ID, clone an activated customer disk as a template, expose database ports, or change the VM clock to extend licensing. Changing a custom portal hostname/certificate requires a coordinated origin/proxy/certificate change; do not rerun first-time preparation over existing secrets.

Basis and limits of this guide

Commands were checked against the OTL appliance startup/setup helpers, PostgreSQL compose deployment, backup and restore utilities and release evidence in this workspace. The full-backup example is an operator procedure assembled from those components; it was not executed against customer production data for this document. Screens and labels may vary slightly by release. Use the delivered package instructions when they differ and confirm with support.

The appliance is separate from the vendor signing service. A customer does not need vendor private keys or public internet to activate via a signed file. Customer internet is only needed if their chosen mail, directory, certificate or update service depends on it. No endpoint agents are installed by this guide.

Support and purchasing: sales@oneticketless.com
Website: https://oneticketless.com