



VDI Access Suite

Administrator Guide

Shell · Agent · Manager

PNQ Software B.V.

October 2026

Contents

1. Introduction	4
1.1 About this guide.....	4
1.2 Components.....	4
1.3 How the components work together.....	4
1.4 Terminology	5
2. VDI Access Suite (shell)	6
2.1 Installation and shell setup	6
2.2 Licensing of the shell.....	6
2.3 The workplace.....	7
2.4 Settings panel.....	7
2.5 Configuration file vas.ini	8
2.6 Secure Web Browser.....	8
3. VDI Access Suite Manager Agent	9
3.1 Installation and configuration.....	9
3.2 Enrollment	9
3.3 Check-in cycle	10
3.4 Profiles	10
3.5 Jobs	10
3.6 Write filters	11
3.7 Updating the Agent.....	11
4. VDI Access Suite Manager.....	12
4.1 Architecture	12
4.2 Signing in and console layout.....	12
4.3 Devices	13
4.4 Groups and profiles.....	14
4.5 Repository	15
4.6 Policies	16
4.7 Jobs	17
4.8 Settings	18
5. Common tasks.....	19
5.1 Preparing a new organization.....	19
5.2 Bringing a device under management	19
5.3 Branding the workplace with a custom wallpaper	19
5.4 Deploying an application	19
5.5 Running a PowerShell script	20
5.6 Restarting, shutting down or locking devices	20
5.7 Updating the Agent.....	20

5.8 Retiring a device.....	20
6. Security	21
7. Licensing.....	21
8. Troubleshooting.....	22
Appendix A. vas.ini reference	23
Appendix B. Agent configuration.....	23
Appendix C. Policy and job actions	23

1. Introduction

1.1 About this guide

This guide describes the installation, configuration and day-to-day administration of VDI Access Suite, the VDI Access Suite Manager Agent and VDI Access Suite Manager. It is intended for system administrators who prepare workplace systems, maintain the central console and support end users.

Chapter 2 covers the shell on the workplace system, chapter 3 the Agent, chapter 4 the Manager console screen by screen, and chapter 5 the most common administrative tasks step by step. Security, licensing, troubleshooting and reference tables follow at the end.

1.2 Components

VDI Access Suite turns a Windows system into a locked-down workplace. The Agent and the Manager keep a fleet of such systems configured and maintained from one central place.

Component	Runs on	Role
VDI Access Suite (vas.exe)	Each workplace system, as the shell of the user	Replaces Windows Explorer: wallpaper, sidebar (taskbar), start menu, application launcher and settings panel
VDI Access Suite Manager Agent	Each workplace system, as a Windows service under SYSTEM	Checks in with the Manager, applies the profile to vas.ini , runs signed jobs and reports inventory and state
VDI Access Suite Manager	Central server (Windows Server, IIS, PostgreSQL)	Web console for devices, groups, profiles, repository, policies and jobs, plus the API the Agents connect to

The shell works without the Agent and the Manager: **vas.ini** can be maintained by hand or with an existing management tool. The Agent and the Manager add central profile management and light system management (software installation, file delivery, scripts and power actions) on top.

The Agent and the Manager manage only systems that have the VDI Access Suite shell installed. The solution runs on any Windows hardware, including thin clients running Windows IoT Enterprise and repurposed PCs.

1.3 How the components work together

1. The Agent is installed on the workplace system and enrolls once with an enrollment token. From then on the device is known in the Manager.
2. The Agent checks in with the Manager over HTTPS. The connection always starts at the device; the Manager never connects to the device.
3. The Manager returns what is waiting for the device: the profile of its group and any jobs created by policies or by administrator actions. Everything is signed with the signing key of the organization.
4. The Agent verifies the signature, writes the profile to **vas.ini**, runs the jobs and reports the results at the next contact.
5. When the profile changed a setting, the Agent restarts **vas.exe** in the user session, so the new configuration is visible within seconds.

1.4 Terminology

Term	Meaning
Device	A workplace system enrolled in the Manager through the Agent.
Group	A container for devices. Groups form a tree under the root group All devices.
Profile	The set of vas.ini keys and values defined on a group. Only the keys in the profile are managed.
Repository item	A file stored in the Manager: an MSI or EXE installer, a PowerShell script or any other file.
Policy	An action devices have to carry out, such as installing software, running a script, placing a file, locking the workstation or restarting. A policy is linked to one or more groups.
Job	One action for one device. Policies and administrator actions on the Devices page create jobs.
Check-in	The regular contact of the Agent with the Manager.
Enrollment token	A token that allows a new device to enroll. Tokens expire and can be revoked.
Signing key	The key pair of the organization. The Manager signs profiles and jobs; every device holds the public key and runs only correctly signed content.
Tenant / organization	A customer environment in the Manager. Administrators see only the data of their own organization.

2. VDI Access Suite (shell)

VDI Access Suite replaces Windows Explorer for the logged-on user, so that only the applications defined in `vas.ini` can be reached. There is no Windows taskbar, Start menu or desktop; the shell provides its own sidebar and application menu instead.



Figure 1. The VDI Access Suite workplace with a custom wallpaper and the sidebar on the left edge

2.1 Installation and shell setup

- **Requirements:** Windows 10 or Windows 11 (including IoT Enterprise LTSC) and the .NET 8 Desktop Runtime.
- **Installation:** for all users, by default in `C:\Program Files\PNQ Software\VDI Access Suite`. The installer can be deployed centrally, for example through a policy in the Manager.
- **Shell replacement:** the Winlogon `Shell` registry value of the intended user is pointed to `vas.exe`. The change applies at the next logon of that user. Other users keep Windows Explorer.
- **Per-user data folder:** `%AppData%\PNQ Software\VDI Access Suite` holds `vas.ini`, the optional wallpaper file and the log file `vas.log`.
- **Closing:** Alt+F4 does not close the shell. Logging off, restarting and shutting down are done from the power menu.

Recommendation Test the shell replacement with a spare account first. A shell that fails to start leaves a black screen; Ctrl+Alt+Delete still offers Sign out.

2.2 Licensing of the shell

A valid license is required. Without one, an activation window opens. For central deployment, a license key placed in `license.ini` is activated silently at startup. With no license or an invalid one, the message "No or invalid license" is shown and, after confirmation, the user is logged off. The application itself is never closed.

2.3 The workplace

The sidebar on the left edge of the primary screen contains, from top to bottom, the Info button, the Start button, the icons of running applications and, at the bottom, Sound, Settings, Power and the clock (see Figure 1).

Element	Behavior
Wallpaper	Shown on every connected screen. A custom image, such as a corporate background, is set with the Wallpaper key in vas.ini .
Sidebar	Slides out from the left edge of the primary screen when the mouse touches the edge and slides away about one second after the mouse leaves. It stays open while a menu or popup is open. With Taskbar = Locked it is always visible and its space is reserved.
Info button	Shows device name, user, IP address, MAC address and serial number. Useful when a user contacts the service desk.
Start button	Opens the application menu with the applications from vas.ini . A short tap on the Windows key opens it as well. Key combinations such as Win+L keep working.
Running applications	One icon per open window. Clicking brings the window to the front, minimizes the active window or restores a minimized one.
Sound	Volume slider for the default output device. The icon in the popup toggles mute.
Settings	Opens the settings panel (section 2.4).
Power	Shutdown, Restart and Log off. Each button can be hidden in vas.ini .
Clock	Time and date.

Application menu. Shows the applications from **vas.ini** with their icons. The Admin button opens an elevated PowerShell after a Windows UAC prompt; it can be hidden with **Admin = Yes** in the **[Hide]** section.

Window switching. Alt+Tab shows a custom switcher with one tile per open window. Titles longer than 40 characters are shortened with an ellipsis. Window title changes (for example a browser navigating to another page) update the sidebar icon and the tile.

Multiple screens. The wallpaper covers all screens. The sidebar appears on the primary screen only.

2.4 Settings panel

Because the Windows Settings app is not reachable, the shell offers its own settings panel:

- **Display:** per monitor, resolution, refresh rate and orientation, plus brightness and contrast through DDC/CI. Brightness and contrast are applied when the slider is released.
- **Mouse:** pointer speed and swapping of the left and right buttons.
- **Sound:** default output and input device, each with a volume slider.

Network, date and time, region and power settings are not offered in this version.

2.5 Configuration file vas.ini

Location: %AppData%\PNQ Software\VDI Access Suite\vas.ini. The file is read when the shell starts, so a change becomes active after the shell restarts. The Agent does this automatically after a profile change. Boolean values accept **Yes** or **True**; any other value counts as No. The complete key reference is in Appendix A.

Example:

```
[Settings]
Wallpaper = company.jpg
Taskbar = Unlocked

[Hide]
Admin = Yes

[App1]
Name = Remote Desktop
Application = C:\Windows\System32\mstsc.exe
Arguments = /v:server01 /multimon
Icon = rdp
Autolaunch = No
```

Several entries may point to the same executable with different arguments (for example several Secure Web Browser kiosks). The sidebar icon then follows the matching entry.

2.6 Secure Web Browser

Secure Web Browser is a separate, license-free browser delivered with the suite and started like any other application through an [AppN] entry. Its executable is **swb.exe** in the Secure Web Browser subfolder of the installation folder.

The arguments can be combined in any order:

Argument	Result
-k or -kiosk	Kiosk mode: full screen, no window frame
-b or -browser	Browser mode: normal window
<URL>	Start URL (must be a complete URL, including https://)
-m	Browser mode: start maximized
-n	Browser mode: start in a normal window (default)
-f or -fresh	Fresh start: cookies, cache, saved logins and autofill data are cleared before the first page loads
-keep=<domain>	Used together with -f : comma-separated sites whose cookies are kept. A listed domain also covers its subdomains. Without -f the option has no effect.

Several instances can run side by side. Settings are kept in **swb.ini** under %AppData%\PNQ Software\VDI Access Suite\Secure Web Browser. Navigation uses the keyboard: **Alt+Left** goes back and **Alt+Right** goes forward.

3. VDI Access Suite Manager Agent

The Agent is a Windows service that runs under the SYSTEM account on every managed workplace system. It is the component that establishes and maintains the connection with the Manager: it enrolls the device, checks in regularly and carries out what the Manager has prepared for it. Without a running Agent, a device cannot be managed remotely.

3.1 Installation and configuration

1. Install the Agent on the workplace system with the Agent setup (for example **vma-Setup-<version>.exe**). The service is registered as VDI Access Manager Agent and starts automatically.
2. In the Agent configuration file (JSON, in the Agent data folder), set the keys of the **Agent** section (see the table below and Appendix B).
3. Start or restart the service. If **ServerUrl** is missing or invalid, the service stops at startup with a clear message in the Windows event log.

Key	Meaning
ServerUrl	Address of the Agent API of the Manager, for example https://api.vdimanager.pnqsoftware.com . Must start with https.
EnrollmentToken	Token created in the Manager under Settings > Enrollment tokens, used for the first enrollment.
AllowInsecureHttp	Permits http for local development only. Never used in production.

The Agent data folder is restricted to SYSTEM and Administrators. It holds the configuration, the stored device identity, the state of processed jobs and the public key used to verify signed content.

Image preparation For larger rollouts the Agent and its configuration file can be included in the system image or deployed with an existing software distribution tool. Every device enrolls with the same token and gets its own identity at first start.

3.2 Enrollment

On the first start the Agent presents the enrollment token together with the machine identifier, host name, model, operating system version, serial number, MAC address and Agent version. The Manager returns a device identifier and a device token. The identity is stored protected with Windows DPAPI. The new device appears on the Devices page, in the root group All devices.

When the Manager rejects the device token (for example after the device was removed in the console), the stored identity is discarded and the Agent enrolls again with the configured token, provided that token is still valid.

3.3 Check-in cycle

- The Agent contacts the Manager over HTTPS. When nothing is waiting, the Manager keeps the request open for a while, so new profiles and jobs arrive almost immediately.
- After a failed attempt the waiting time grows from 30 seconds up to 10 minutes. A random delay of up to 60 seconds is added between cycles, so a fleet does not call in at the same moment.
- Each check-in reports the Agent version, the write filter state, the license state, the applied profile and whether the device complies with it, the results of finished jobs and an inventory: host name, model, operating system, IP addresses, serial number, MAC address and a hash of the installed software. The full software list is sent only when the Manager asks for it.

The time of the last check-in is shown in the Last seen column of the Devices page. A device is shown as online while it keeps contact and as offline when the contact has stopped, for example because the system is switched off.

3.4 Profiles

A profile lists the `vas.ini` keys that must have a specific value. The Agent:

1. verifies the signature of the profile;
2. applies it at every check-in, also when nothing new arrived, so manual changes to managed keys are repaired;
3. changes only the keys listed in the profile and leaves all other settings untouched;
4. keeps the previous version next to the file as `vas.ini.bak` and writes the new file in one atomic step;
5. restarts the shell when something actually changed: the running `vas.exe` is terminated and started again in the active user session, so the new settings are active within seconds. If `vas.exe` is not running, nothing is started.

The applied profile and the compliance state are visible per device in the Profile column of the Devices page.

3.5 Jobs

Jobs are actions prepared in the Manager, such as installing software, running a PowerShell script, placing a file, locking the workstation, restarting or shutting down. The Agent runs a job only when:

- the signature is valid;
- the job is meant for this device;
- the job has not expired (judged by the server time, so a wrong clock on the device does not matter);
- the job has not been run before. A job is recorded as processed before it starts, so a crash can never lead to a second run.

Before a repository file is used, the Agent checks that it is exactly the file that was uploaded to the Manager; a modified or incomplete download is rejected. Actions that must be visible to the user, such as locking the screen, are started inside the interactive user session instead of the SYSTEM session. The result of each job, including the exit code and output, is reported at the next contact, usually immediately in a second round.

3.6 Write filters

On thin clients with a write filter (Unified Write Filter), changes to the disk, including `vas.ini` and installed software, can be lost at restart. The state of the write filter is reported with every check-in and shown in the Write filter column of the Devices page (`none`, `off` or `on`), so affected devices can be recognized before changes are rolled out.

3.7 Updating the Agent

The Agent can update itself through the Manager: the new Agent setup is added to the Repository as an application and installed with a policy on the intended groups. The Agent version of every device is visible in the Agent column of the Devices page (see section 5.7).

4. VDI Access Suite Manager

VDI Access Suite Manager is the central web console for managing workplace systems that run the VDI Access Suite shell. It is a lighter alternative to vendor-specific management suites and works with any Windows hardware.

4.1 Architecture

- **Web console:** ASP.NET Core application for administrators, opened in a web browser (for example <https://vdimanager.pnqsoftware.com>).
- **Agent API:** a separate endpoint on its own address (for example <https://api.vdimanager.pnqsoftware.com>), used only by the Agents.
- **Database:** PostgreSQL. Customers are separated as organizations (tenants); an administrator sees only the data of the own organization.
- **Hosting:** Windows Server with IIS. The console and the Agent API run in separate application pools.

4.2 Signing in and console layout

After signing in, the console shows a navigation menu on the left with the pages Devices, Groups, Repository, Policies, Jobs and Settings. The bar at the top right shows:

Item	Purpose
Organization name	The organization (tenant) currently managed, for example PNQ Software.
User and role	The signed-in account and its role, for example Team Support (Admin).
Security	Security settings of the own account, such as sign-in protection.
Password	Changes the password of the own account.
Sign out	Ends the session.
Dark mode	Switches between the dark and the light theme of the console.

4.3 Devices

The Devices page lists every enrolled device with its group, hardware and last known state.

Figure 2. Devices page with bulk actions and the device list

Counters. Four tiles at the top show the total number of devices, the number online, the number offline and the number of devices on which the profile is not applied. The last tile is the quickest indication that something needs attention.

Search and filter. The search box searches on host name, model, serial number and other device data. The drop-down narrows the list by state (for example all devices, online, offline or profile not applied). Filter applies the selection.

Columns

Column	Meaning
Host name	Name of the device. The link opens the device details.
Group	Group the device is in. This determines the profile and the policies that apply.
Model / Serial number / MAC address	Hardware data reported by the Agent.
Operating system	Windows edition, version and build.
Agent	Version of the installed Agent.
Write filter	State of the write filter: none (not present), off or on.
Profile	applied when vas.ini matches the profile of the group; otherwise the device is not compliant.
Last seen	Online or offline, with the time of the last check-in.

Actions

Select one or more devices with the check boxes, then choose an action:

- **Restart, Shutdown and Lock workstation** create a job per selected device. The job runs at the next check-in; the result appears on the Jobs page.
- **Move to group with Move** places the selected devices in another group. Each device picks up the profile of its new group, and the policies that apply there, at the next check-in.

Note Actions on an offline device wait until the device checks in again. A Restart or Shutdown on a device in use interrupts the session of the user.

4.4 Groups and profiles

Devices are placed in groups. Groups form a tree under the root group All devices, so the structure can follow customers, locations, departments or test and production environments.

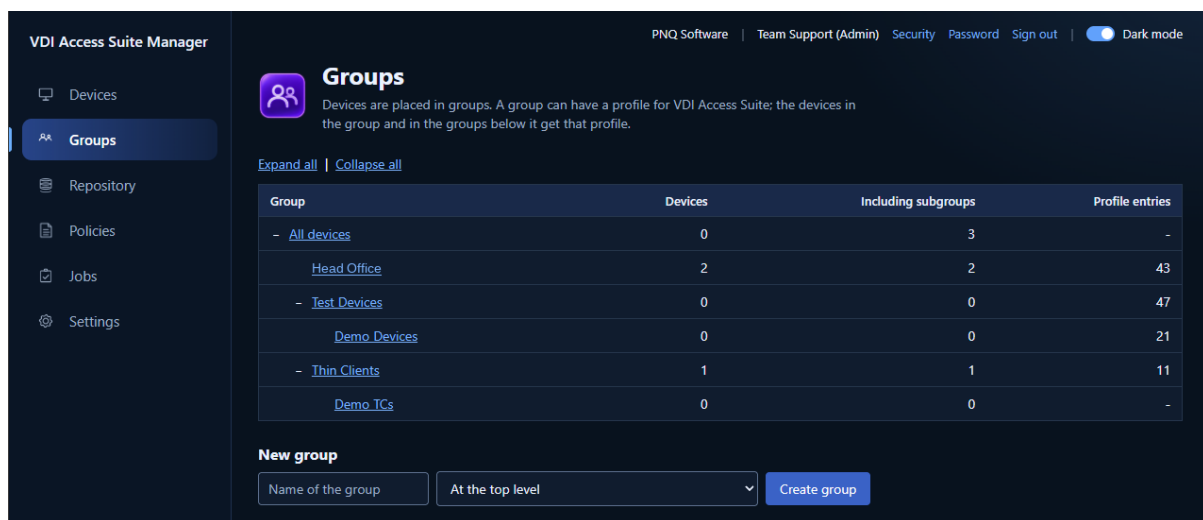


Figure 3. Groups page with a group tree and the number of profile entries per group

Column	Meaning
Group	Name of the group. The link opens the group with its profile. The - sign collapses a branch; Expand all and Collapse all act on the whole tree.
Devices	Devices placed directly in this group.
Including subgroups	Devices in this group and in all groups below it.
Profile entries	Number of vas.ini keys defined in the profile of this group; - means the group has no profile of its own.

Creating a group. Under New group, enter the name, choose the parent group (or At the top level) and select Create group.

Profiles

A group can have a profile for VDI Access Suite. The profile applies to the devices in the group and in the groups below it. A profile consists of **vas.ini** entries, each a section, a key and a value, for example **[Settings] Wallpaper = company.jpg** or a complete **[App1]** application entry. INI section and key names are entered exactly as listed in Appendix A.

- Only the keys in the profile are managed on the device. All other keys in **vas.ini** stay under local control.
- A changed profile is signed and delivered at the next check-in. Devices on which a setting changed restart the shell automatically.
- Keeping a test group (for example Test Devices with a few representative systems) allows a profile change to be verified before it is applied to production groups.

4.5 Repository

The Repository holds the files that policies use: installers, scripts and other files. A device only receives a file when a policy asks for it, and only uses it when it is exactly the file that was uploaded.

Repository
The files that policies use: installers, scripts and other files. A device only receives a file when a policy asks for it, and only uses it when it is exactly the file that was uploaded.

Application install
Deploy and manage MSI and EXE installers on devices.

File delivery
Distribute files, configuration and resources.

PowerShell scripts
Run scripts on endpoints, for example for updates or configuration.

Group-based profiles
Use device groups to create dedicated VDI Access Suite profiles.

Repository items 16 items [+ Add file](#)

Name	Version	Type	Size	Uploaded	Used by	Status
ChromeEnterprise GoogleChromeStandaloneEnterprise64.msi	154.0.8037.58	MSI	159.9 MB	8 d ago by Team Support	1 policy	In use
CitrixWorkspaceApp CitrixWorkspaceApp_x64.exe	2603.11	EXE	461.8 MB	8 d ago by Team Support	1 policy	In use
Create Admin CreateAdmin.ps1	1.0	PowerShell	1.1 KB	6 d ago by Team Support	-	Not in use
Create VAS User CreateVasUser.ps1	1.1	PowerShell	14.3 KB	6 d ago by Team Support	-	Not in use
Firefox Firefox Setup 156.0.1.msi	156.0.1	MSI	88.6 MB	8 d ago by Team Support	1 policy	In use
Hide Drive C:\ HideDriveC.ps1	1.0	PowerShell	2.2 KB	18 h ago by Team Support	1 policy	In use
Libre Office LibreOffice_26.8.0_Win_x86-64.msi	26.8	MSI	357.5 MB	7 d ago by Team Support	1 policy	In use
Omniissa-Horizon-Client Omniissa-Horizon-Client-2606-8.19.0-32215843441.exe	2606-8.19.0	EXE	341.7 MB	8 d ago by Team Support	1 policy	In use
Power Options System Sleep Off PowerOptionsSleepOff.ps1	1.0	PowerShell	364 B	6 d ago by Team Support	1 policy	In use
ScreenGenie ScreenGenie.msi	26.7.3230	MSI	243.8 MB	6 d ago by Team Support	1 policy	In use
VDI Access Suite Manager Agent vma-Setup-26.10.309.0.exe	26.10.0909	EXE	25 MB	42 h ago by Team Support	1 policy	In use
Wallpaper 1 WP1.png	1.0	File	40.2 MB	6 d ago by Team Support	1 policy	In use
Wallpaper 4 WP4.jpg	1.0	File	1.1 MB	17 h ago by Team Support	1 policy	In use
Windows 11 Blue Wallpaper windows-11-blue-3840x2400-11776.png	1.0	File	9.4 MB	7 d ago by Team Support	1 policy	In use

Quick actions

- Add application**
Upload an MSI or EXE installer
- Add file**
Distribute files to devices
- Add PowerShell script**
Upload a .ps1 script
- Manage groups**
Create profiles for device groups

Repository usage

16 items

- Applications: 7
- PowerShell scripts: 5
- Files: 4

Recent activity

- Wallpaper 4
File added 17 h ago
- Hide Drive C:\
Script added 18 h ago
- WP2
File added 25 h ago
- VDI Access Suite Manager Agent
Application added 42 h ago

Figure 4. Repository page with items, quick actions, usage and recent activity

The tiles at the top describe the four main uses: Application install (MSI and EXE installers), File delivery (files, configuration and resources), PowerShell scripts, and Group-based profiles.

Column	Meaning
Name	Display name and original file name.
Version	Version of the item, used in policy names and results.
Type	MSI, EXE, PowerShell or File.
Size / Uploaded	File size, upload time and the account that uploaded it.
Used by	Number of policies that use the item. The link shows them.
Status	In use when at least one policy uses the item, otherwise Not in use.
: menu	Further actions on the item.

Adding items. Add file, or the Quick actions Add application, Add file and Add PowerShell script, upload a new item. Manage groups opens the Groups page. The Repository usage panel shows the number of applications, scripts and files; Recent activity lists the latest additions. The search box finds items by name or file name.

Tip An item that is still used by a policy is marked In use. Before an item is replaced or removed, the policies that use it are best updated first.

4.6 Policies

A policy is something devices have to do: install or remove software, run a script, place a file, lock the workstation or restart. A policy is linked to one or more groups and applies to all devices in those groups and in the groups below them.

Policy	What	File	Schedule	Groups	Result (this version)
Citrix WorkspaceApp_2603.11	Install	CitrixWorkspaceApp 2603.11	Until it succeeds	-	1 done
Firefox_156.0.1	Install	Firefox 156.0.1	Until it succeeds	-	no results yet
Google.Chrome_154.0.8037.58	Install	ChromeEnterprise 154.0.8037.58	Until it succeeds	-	1 done
Hide Drive C:\VAS Demo	Run script	Hide Drive C:\ 1.0	Until it succeeds	1	1 done
HorizonClient-2606-8.19.0	Install	Omniissa-Horizon-Client 2606-8.19.0	Until it succeeds	-	1 done
Libre Office 26.8 scheduled	Install	Libre Office 26.8	Until it succeeds	1	no results yet
Lock Windows Desktop	LockWorkstation	-	Until it succeeds	-	1 done
Power.Options System Sleep Never	Run script	Power Options System Sleep Off 1.0	Until it succeeds	-	1 done
Restart	Restart	-	Until it succeeds	-	no results yet
ScreenGenie_26.7.3230	Install	ScreenGenie 26.7.3230	Until it succeeds	-	1 done
VDI.Access.Suite.Manager.Agent	Install	VDI Access Suite Manager Agent 26.10.0909	Until it succeeds	-	no results yet
Wallpaper_1	Place file	Wallpaper 1 1.0	Until it succeeds	-	1 done
Wallpaper_2	Place file	WP2 1.0	Until it succeeds	1	1 done
Wallpaper_4	Place file	Wallpaper 4 1.0	Until it succeeds	1	1 done
Windows 11 Blue Wallpaper	Place file	Windows 11 Blue Wallpaper 1.0	Until it succeeds	-	1 done
Windows Update	Run script	Windows Update 2.0	Until it succeeds	-	no results yet

Figure 5. Policies page with the action, file, schedule, linked groups and results of each policy

Column	Meaning
Policy	Name of the policy. The link opens it for editing. A scheduled label means the policy starts at a set moment instead of immediately.
What	The action: Install , Uninstall , Run script , Place file , LockWorkstation or Restart .
File	The repository item used, with its version (- for actions without a file).
Schedule	How often the policy is carried out, for example Until it succeeds : each device keeps getting the job until it has completed successfully once.
Groups	Number of groups the policy is linked to. A policy without groups (-) does nothing.
Result (this version)	Results of the current version of the policy, for example 1 done , or no results yet when no device has reported back.

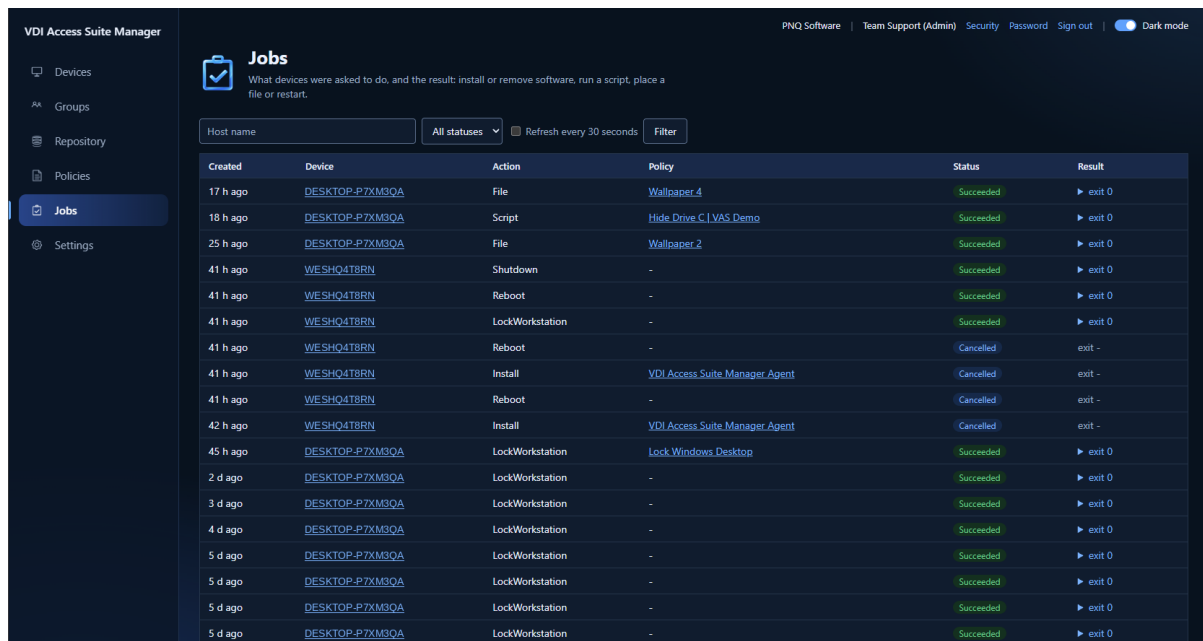
New policy creates a policy: choose the action, the repository item where applicable, the schedule (immediately or at a later moment) and the groups. As soon as a policy is linked to a group, a job is

created for each device in that group and its subgroups; devices that join the group later get the job as well.

Note Results are counted per version of the policy. When a policy is changed, for example to point to a newer installer, devices carry it out again and the result count starts anew.

4.7 Jobs

The Jobs page shows what devices were asked to do and the result: install or remove software, run a script, place a file, lock, restart or shut down.



Created	Device	Action	Policy	Status	Result
17 h ago	DESKTOP-P7XM3QA	File	Wallpaper 4	Succeeded	exit 0
18 h ago	DESKTOP-P7XM3QA	Script	Hide Drive C VAS Demo	Succeeded	exit 0
25 h ago	DESKTOP-P7XM3QA	File	Wallpaper 2	Succeeded	exit 0
41 h ago	WESHQ4T8RN	Shutdown	-	Succeeded	exit 0
41 h ago	WESHQ4T8RN	Reboot	-	Succeeded	exit 0
41 h ago	WESHQ4T8RN	LockWorkstation	-	Succeeded	exit 0
41 h ago	WESHQ4T8RN	Reboot	-	Cancelled	exit -
41 h ago	WESHQ4T8RN	Install	VDI Access Suite Manager Agent	Cancelled	exit -
41 h ago	WESHQ4T8RN	Reboot	-	Cancelled	exit -
42 h ago	WESHQ4T8RN	Install	VDI Access Suite Manager Agent	Cancelled	exit -
45 h ago	DESKTOP-P7XM3QA	LockWorkstation	Lock Windows Desktop	Succeeded	exit 0
2 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
3 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
4 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
5 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
5 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
5 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0
5 d ago	DESKTOP-P7XM3QA	LockWorkstation	-	Succeeded	exit 0

Figure 6. Jobs page with the status and exit code of every job

Column	Meaning
Created	When the job was created.
Device	The device. The link opens the device details.
Action	Install, File, Script, LockWorkstation, Reboot or Shutdown.
Policy	The policy that created the job, or - for an action started from the Devices page.
Status	For example Succeeded or Cancelled; jobs that are still waiting or running and jobs that failed are shown with their own status.
Result	Exit code of the action. Expanding the row shows the output reported by the Agent.

The list can be narrowed by host name and status. With Refresh every 30 seconds selected, the page updates itself, which is useful while a rollout is in progress.

Exit codes Exit code 0 means success. For MSI installations, 3010 means success with a restart required. Other values point to an error; the output of the job and the log of the installer give the details.

4.8 Settings

Settings covers the organization, its license, enrollment tokens, users, the signing key and the audit log. The Overview tab summarizes each part; the other tabs open the details.

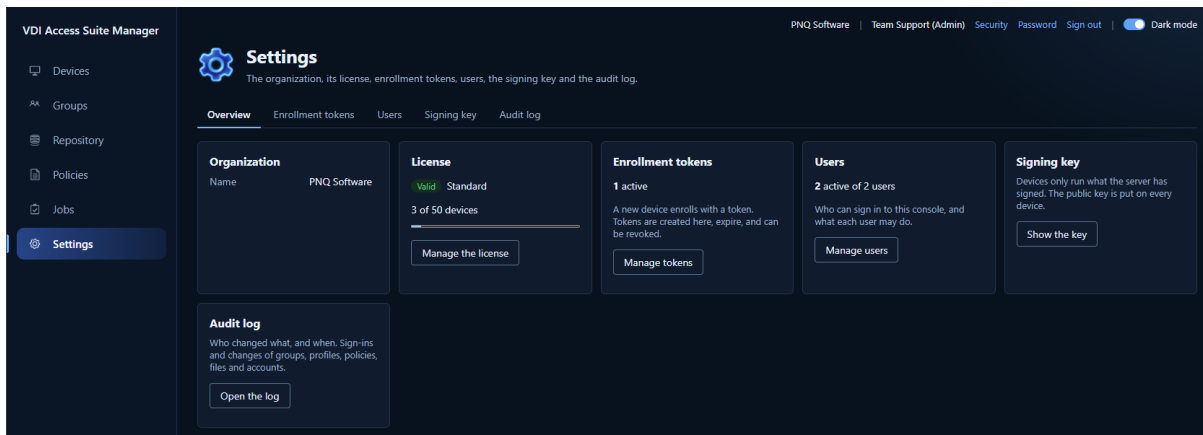


Figure 7. Settings overview

Part	Purpose
Organization	Name of the organization (tenant).
License	License state and edition (for example Valid, Standard) and the number of devices in use against the licensed number. Manage the license enters or renews the license.
Enrollment tokens	Tokens with which new devices enroll. Tokens are created here, have an expiry date and can be revoked. Revoking a token does not affect devices that already enrolled with it.
Users	The accounts that can sign in to the console and what each account may do. Accounts can be deactivated without being removed.
Signing key	Devices only run what the server has signed. The public key is placed on every device; Show the key displays it, for example for verification.
Audit log	Who changed what, and when: sign-ins and changes to groups, profiles, policies, files and accounts.

Recommendation Use a personal account for each administrator and deactivate accounts of people who leave. The audit log then shows exactly who made each change.

5. Common tasks

5.1 Preparing a new organization

1. Sign in to the console and check the license under Settings > License.
2. Under Settings > Users, create an account for each administrator.
3. On the Groups page, create the group structure, for example one group per location plus a test group.
4. Define a profile for each group that needs specific **vas.ini** settings.
5. Under Settings > Enrollment tokens, create a token with a suitable expiry date.

5.2 Bringing a device under management

1. Install the VDI Access Suite shell and set it as the shell of the intended user (section 2.1).
2. Install the Agent and put the server address and the enrollment token in its configuration (section 3.1).
3. Start the Agent service. The device appears on the Devices page, in All devices, within a few minutes.
4. Select the device, choose the target group under Move to group and select Move.
5. At the next check-in the profile of the group is applied, the shell restarts when a setting changed, and the policies of the group are carried out. The Profile column then shows **applied**.

5.3 Branding the workplace with a custom wallpaper

1. Add the image (PNG or JPG) to the Repository with Add file.
2. Create a policy with the action Place file that places the image next to **vas.ini** of the shell user, and link it to the group.
3. In the profile of the same group, add **[Settings] Wallpaper** with the file name of the image as value.
4. At the next check-in the file is placed, the profile is applied and the shell restarts with the new wallpaper (see Figure 1).

5.4 Deploying an application

1. Upload the MSI or EXE installer with Add application on the Repository page.
2. Create a policy with the action Install, select the repository item and, for an EXE, the silent installation arguments.
3. Link the policy first to a test group and follow the result on the Jobs page.
4. When the installation succeeds, link the policy to the production groups.
5. Add an **[AppN]** entry to the profile so the application appears in the application menu of the shell.

Write filter On devices with an enabled write filter, an installation is lost at the next restart. The write filter has to be disabled first, or the change committed, before software is installed.

5.5 Running a PowerShell script

1. Upload the `.ps1` file with Add PowerShell script.
2. Create a policy with the action Run script and link it to the intended groups.
3. Check the exit code and the output on the Jobs page. A script signals failure with a non-zero exit code (for example `exit 1`).

Scripts run under the SYSTEM account. Typical uses are power settings, local accounts, hiding drives or starting Windows Update.

5.6 Restarting, shutting down or locking devices

On the Devices page, select the devices, then Restart, Shutdown or Lock workstation. For a recurring or group-wide action, a policy with the action Restart or LockWorkstation can be used instead, optionally scheduled for a later moment (for example outside office hours).

5.7 Updating the Agent

1. Upload the new Agent setup with Add application.
2. Create or update the Install policy for the Agent and link it to a test group.
3. Check the Agent column on the Devices page; when the test devices report the new version, link the policy to the other groups.

5.8 Retiring a device

Remove the device in the console. Its device token becomes invalid immediately and the device can no longer receive profiles or jobs. If the Agent is still installed with a valid enrollment token, the device enrolls again as a new device; for permanent retirement the Agent is uninstalled as well.

6. Security

- All communication between Agent and Manager uses HTTPS. The Agent always initiates the connection; no inbound ports are needed on the devices.
- Every device has its own device token. A removed device loses access immediately.
- Profiles and jobs are signed with the signing key of the organization. The Agent rejects content with an invalid signature, content meant for another device and expired content.
- Repository files are verified on the device and used only when they are identical to the uploaded file.
- Jobs run at most once per device.
- The Agent data folder is accessible to SYSTEM and Administrators only; the device identity is protected with DPAPI.
- Enrollment tokens expire and can be revoked, so a leaked token has limited value.
- Administrator accounts have their own roles; every sign-in and change is recorded in the audit log.
- Organizations (tenants) are strictly separated in the Manager.

7. Licensing

The shell and the Manager each carry their own license.

- **Shell:** licensed per workplace system (section 2.2).
- **Manager:** licensed per managed device. Settings > License shows the edition and the number of devices in use against the licensed number (for example 3 of 50 devices).
- When the Manager license ends, enrolled devices keep working for at most 14 days. After that, management stops until the license is renewed. The shell itself keeps working with its own license.

8. Troubleshooting

The shell writes diagnostics to `%AppData%\PNQ Software\VDI Access Suite\vas.log` (one line per event, with timestamp). The Jobs page shows the exit code and output of every job, and the audit log shows recent changes in the console.

Symptom	Likely cause	Action
Black screen after logon	The shell failed to start or the registered path is wrong	Sign out with Ctrl+Alt+Delete, check the Shell registry value and the installation folder, then sign in again
"No or invalid license" message	License missing, expired or bound to other hardware	Activate with a valid key (activation window or license.ini)
Sidebar does not slide out	Mouse does not touch the left edge of the primary screen	Move the mouse against the very edge; check the Taskbar value
Application missing in the menu	Entry has no Name or the Application path is wrong	Correct the [AppN] section in the profile or vas.ini
Wrong or generic icon	Icon value not recognized	Use one of the named icons or a valid image path
Change in vas.ini has no effect	The file is read at shell start only	Restart the shell or sign out and in again; with the Agent this happens automatically
Device does not appear in the console	Wrong ServerUrl , expired or revoked token, or outbound HTTPS blocked	Check the Agent configuration, the service state and outbound access to the Agent API
Device shows as offline	System switched off, network down or Agent service stopped	Check the system and the service; actions wait until the next check-in
Profile not applied	vas.ini is not writable or is reset by a write filter	Check file permissions and the Write filter column of the device
Shell does not restart after a profile change	vas.exe was not running in an interactive session at that moment	Restart the shell manually; the new profile is already in vas.ini
Previous settings needed back	A profile applied unwanted values	Restore vas.ini.bak next to vas.ini and correct the profile
Policy shows "no results yet"	Policy not linked to a group, group without devices, devices offline, or a scheduled start not reached yet	Check the Groups column of the policy and the state of the devices
Job failed or non-zero exit code	Installer or script error, missing silent arguments or an active write filter	Expand the result on the Jobs page, correct the policy and let it run again
Job cancelled	The job was withdrawn, for example because the policy changed or the device left the group	No action needed; a current job is created when the policy still applies

Appendix A. vas.ini reference

Section	Key	Meaning
[App1] ... [AppN]	Name	Label of the application. An entry without Name is ignored.
	Application	Full path of the executable.
	Arguments	Command-line arguments (optional).
	Icon	Named icon (Browser , calc , chrome , citrix , edge , firefox , horizon , notepad , rdp , teams) or the path of an image file. Without a value, the icon of the executable is used.
	Autolaunch	Yes starts the application when the shell starts.
[Hide]	Admin, LogOff, Restart, Shutdown	Yes hides the corresponding button.
[Settings]	Wallpaper	File name of a PNG or JPG placed next to vas.ini .
	Taskbar	Unlocked (default): sidebar slides out on hover. Locked : always visible, space reserved.

Appendix B. Agent configuration

JSON configuration file in the Agent data folder, section **Agent**:

```
{
  "Agent": {
    "ServerUrl": "https://api.vdimanager.pnqsoftware.com",
    "EnrollmentToken": "<token from Settings > Enrollment tokens>"
  }
}
```

Key	Required	Meaning
ServerUrl	Yes	Address of the Agent API; https only.
EnrollmentToken	For enrollment	Token for the first enrollment and for re-enrollment after removal.
AllowInsecureHttp	No	Permits http; for local development only.

Appendix C. Policy and job actions

Policy action (What)	Job action	Repository item	Runs in
Install	Install	MSI or EXE	SYSTEM
Uninstall	Uninstall	MSI or EXE	SYSTEM
Run script	Script	PowerShell	SYSTEM
Place file	File	File	SYSTEM
LockWorkstation	LockWorkstation	-	User session
Restart	Reboot	-	SYSTEM
- (Devices page)	Shutdown	-	SYSTEM

