



Oryx LockDown

Dedicated Windows workspace software

A dedicated workspace built around approved apps

Dedicated workspace · Approved apps · Administrator authentication and recovery



Restrict access to Windows
Run apps in a dedicated workspace

Illustrative image

Dedicated workspace · Approved apps · Administrator authentication

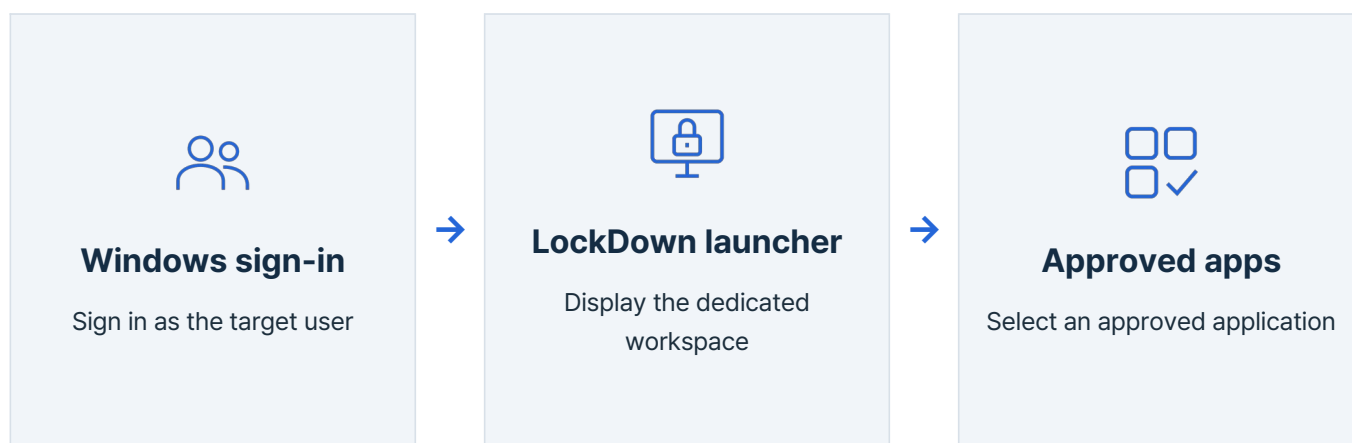
Launcher-based control after Windows sign-in

Product overview

A dedicated workspace after sign-in

The LockDown launcher replaces the standard desktop.

Operators select and launch the applications they need from this workspace.



A workspace for each user

LockDown replaces the target user's Explorer shell with its launcher. The shell is the default workspace displayed after sign-in.

The starting point for daily work

The launcher loads the approved app list saved by the administrator. Operators select and launch the applications they need.

Runs in the signed-in console session

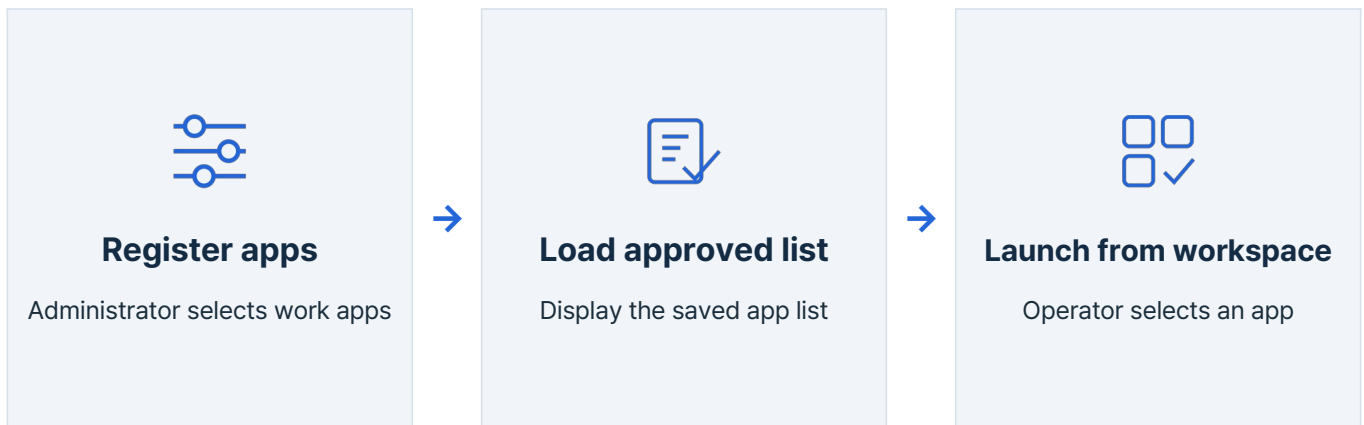
Configuration is based on the session signed in directly on the PC. Confirm the account, sign-in method and on-site workflow before deployment.

A dedicated user workspace and key access restrictions are applied. Review administrator recovery and sign-in after a restart before deployment.

Approved apps and access restrictions

Configure apps and access routes

Manage work applications through an approved list and restrict key Windows access routes to suit on-site operating needs.



Key access routes restricted by configuration

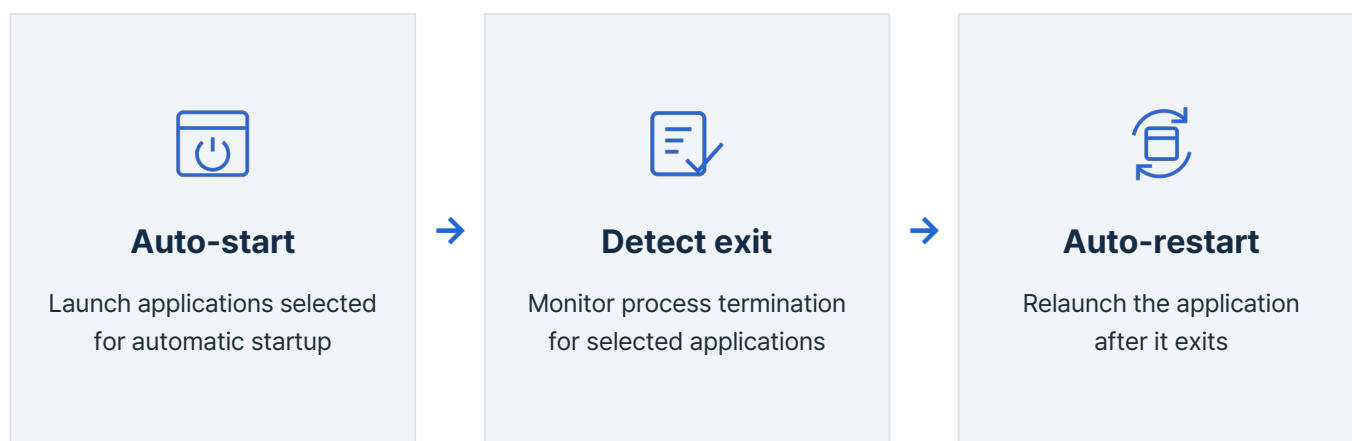
Access route	Control
Standard desktop	Replace the user shell with the dedicated launcher
Windows key · Alt+Tab	Restrict the key or app-switching shortcut
Task Manager	Restrict access to the management interface
Run dialog	Restrict access to the application launch dialog

App control is based on the launcher's registered list. It does not guarantee OS-wide blocking of unregistered executables or every possible bypass.

Automatic startup and restart

Start and relaunch work applications

Automatic startup and restart after an application exits reduce repetitive launch tasks in the dedicated workspace.



Choose how each app operates

Select which applications start automatically and which restart after exiting, according to the on-site workflow.

Restart triggered by process exit

Selected applications can restart automatically after their process exits. Forced termination of unresponsive applications is not included.

Check equipment-linked apps first

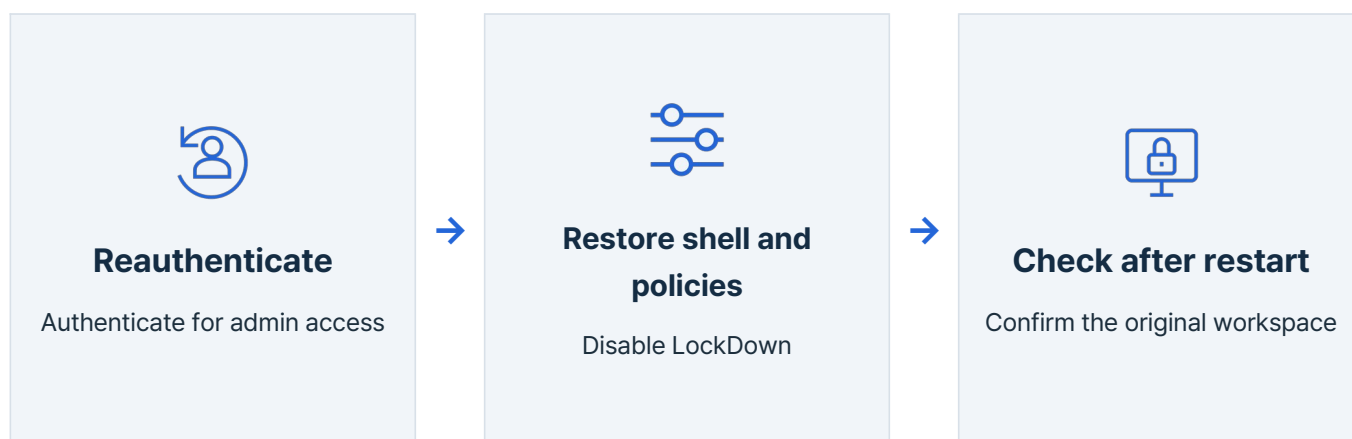
Before enabling restart for PLC/HMI or other equipment-linked apps, verify how communications recover and how operating states are handled.

Auto-restart relaunches applications. It does not guarantee uninterrupted equipment operation or recovery from every failure. Validate each target app.

Administrator authentication and recovery

Restore access with administrator control

Access restrictions remain in place during operation. After reauthentication, administrators can manage settings and restore the original Windows shell.



Authenticate to use admin functions

Administrators reauthenticate before managing settings or disabling LockDown.

Restore the original shell and policies

Disabling LockDown restores the original shell and related policies. Schedule work completion and checks around the recovery procedure, which includes a restart.

Password recovery through support

If an administrator password needs recovery, use the recovery authentication process provided by the support team.

View audit trails and export to PDF

View the Audit Trail and export it to PDF.

Verify restoration and post-restart sign-in on the target PC. Define how administrator credentials are managed and who is responsible for recovery.

Roles of complementary solutions

Separate roles for each solution

LockDown controls access to the Windows workspace.

Data management and equipment control are provided by separate solutions.

	Oryx LockDown Workspace access control	Dedicated workspace · Approved apps Key access restrictions · Admin recovery
	Oryx DataStation Equipment data management	Equipment data collection · Record review Reports and audit history management
	PLC / HMI applications Equipment operation and control	Operator interface · Control logic Communication with on-site equipment

Add the work apps you need

When using DataStation or PLC/HMI applications, review executable paths and permissions before configuring the approved app list.

Validate integration for each project

Data exchange between applications, equipment communications and restart behavior are separate considerations. Verify them on the target PC with the actual work apps.

During deployment, define the scope and responsible solution for PC access, data management and equipment control.

Deployment requirements and checks

Start with the PC and operating procedures

Confirm installation requirements, then test launching, restrictions and recovery with the intended accounts and apps to define the deployment scope.

Item	Current requirement
Installation permissions	Administrator privileges required
System architecture	x64
Installer minimum OS build	10.0.26100 / Windows 11 24H2
Environment to evaluate	Windows IoT Enterprise LTSC
Target user	Target user in the signed-in console session

The minimum build above is required by the installer.

For each Windows edition, including LTSC, separately check the minimum build and on-site compatibility.

Pre-deployment checklist

- 01 Account and sign-in Target account · Sign-in after restart · Launcher display
- 02 Apps and devices Permissions · USB and PLC communication · End-to-end workflow
- 03 Restart and recovery App relaunch · Shell restoration · Restart procedure
- 04 Operational checks Continuous operation · Incident response · Handover

These checks are for pre-deployment validation. They do not indicate completed testing for extended operation or any specific equipment environment.

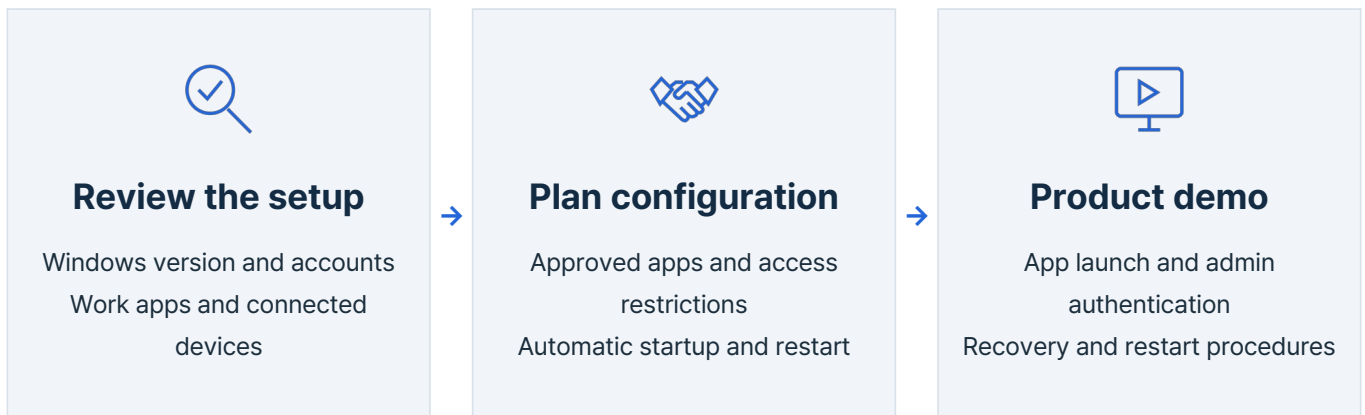
Review the site and operating needs together

Find the right setup for your site

Review the deployment scope and recovery procedure based on your PCs, work applications and operator workflows.



LockDown, data management and equipment control solutions are configured separately for their respective roles.



Features and deployment conditions are confirmed for the product version and site configuration.

Consultation and demo

Seungchul Hong · CEO

010-6545-0415

schong@oryxsystem.co.kr