WHITE PAPER 04 / TEMPORARY ACCESS

Governing Temporary and Privileged Access

Plan the full access window, from justified request and approval to verified expiry and exception handling.

AIdentX Editorial | September 2026

Executive summary

Temporary access should have a clear business purpose and a clear ending. Privileged access deserves particular care because it can change systems, permissions or sensitive information. This paper explains how to govern the whole access window, including maintenance work, supplier support, emergency use and failed revocation. It separates the decision to allow access from the mechanisms that grant and end it.

What you will take away

- Limit the account, permission, system and time window.
- Approve extensions as new decisions rather than silent renewals.
- Verify that expiry ends effective access, not just the request record.

Written for service owners, support teams and privileged-access reviewers.

The worked scenarios are fictional. The checklists and examples are practical editorial guidance, not customer results or audited implementations.

1. Define the work to be done

Just-in-time access means making a permission available for a specific need rather than leaving it continuously assigned. It does not mean that every request should be approved immediately. The request still needs a purpose, appropriate authority and a defined scope.

> **Illustrative workplace case**
>
> Westhaven Logistics is a fictional operator scheduling a supplier to repair a warehouse application. The engineer needs elevated access for a maintenance window. The service owner wants the work completed without leaving a standing administrator account after the supplier finishes.

Describe the task before selecting the permission. Does the engineer need to inspect logs, restart a service or change configuration? A broad administrator role may be convenient, but it can authorise more than the task requires. Where the target application offers only broad permissions, record that limitation and decide how the work will be supervised.

NIST SP 800-207 describes a resource-focused approach to access and rejects implicit trust based solely on network location or ownership. For temporary access, this supports checking the particular request rather than assuming an existing connection is enough. NIST SP 800-207: Zero Trust Architecture.

2. Approve an explicit access window

Record the requester, named user, target system, permission, justification and start and end conditions. The person asking for work is not always the person who will use the access. Avoid an approval that names only a supplier company when several engineers may act.

Request detail	Why it matters
Business task	Allows the owner to judge whether the access is necessary.
Named identity and sponsor	Keeps responsibility attached to a person and internal owner.
Target and permission	Limits where the approved work can occur.
Time window	Defines when the access should become usable and stop.
Conflict or exception	Identifies additional review required before activation.

Define who can approve the permission and who covers their absence. Approval should remain connected to the actual application or business process. An unrelated manager may know the requester but not understand the consequences of elevated access.

At Westhaven, approval covers one warehouse application and one maintenance window. If the engineer later needs production database access, that is a different scope and should not be silently included in the original approval.

3. Confirm activation and operating boundaries

After approval, confirm that the intended access was granted to the correct account. Record the effective start time and the result of the target-system change. A successful request workflow does not guarantee that the engineer has the intended permission or that a broader permission was not granted.

Determine which system handles privileged sessions, logging and termination. Governance, authentication and privileged-session control have related but distinct responsibilities. Document how they connect in the deployed environment, including what happens if a component is unavailable.

IGAX's website describes temporary access, time-limited privileged access, automatic revocation and privileged-session monitoring. Implementation planning should establish which connected systems perform each action and verify the supported behaviour for the selected application. IGAX platform capabilities.

Use approved operational procedures for monitoring. Decide who reviews unusual activity and what information they need. Avoid collecting session material without a defined purpose, access restriction and retention arrangement. These are deployment decisions, not consequences that follow automatically from enabling a request form.

4. Handle extensions and emergency access

Maintenance work sometimes runs longer than expected. An extension should identify the unfinished task, the new end time and the approving authority. Do not let repeated extensions turn temporary access into an informal standing entitlement.

Emergency access needs a prepared process. Decide which situations justify it, who may invoke it, how the activity is recorded and when the use is reviewed. Test the process before an incident. A procedure that depends on an unavailable approver or broken identity service may fail when it is most needed.

Situation	Required decision
Work finishes early	End access through the authorised process rather than wait unnecessarily.
Work exceeds the window	Approve or reject a specific extension.
Different task becomes necessary	Reassess scope and permissions.
Emergency path used	Review the authority, activity and restoration of normal controls.

Keep the original approval and later changes distinguishable. The review should show what was initially authorised and why the final window differed. Replacing the original end time without a history weakens that explanation.

5. Verify the ending

Expiry is a control outcome, not merely a timestamp in a database. Check whether the permission was removed in the target system and whether other assignments still provide equivalent access. Depending on the application, existing sessions or tokens may require separate handling.

Test a failed revocation while the system is being introduced. The exception should identify the account, target, intended end time and owner responsible for restoring the approved state. The response may require an operational action outside the governance tool.

For Westhaven, completion includes evidence that the supplier’s elevated entitlement ended and that any required session termination occurred. The maintenance ticket can then refer to the access record. Retaining a supplier identity for future work is a separate decision from leaving its privileged permissions active.

- The end event was processed at the intended time.
- The target-system entitlement state was checked.
- Equivalent access through another path was considered.
- Failed removals have an owner and escalation.
- Remaining exceptions have a clear next review condition.

6. Review the pattern, not only individual requests

Look for repeated extensions, frequent emergency use and users who require privileged access for nearly every task. These patterns may reveal an unsuitable role design, a maintenance-process problem or an application that lacks sufficiently narrow permissions.

Measure the approved duration and verified duration separately. Review how often access remains active beyond the authorised window and why. Do not hide a significant exception inside an average that combines ordinary low-impact requests with privileged maintenance access.

A useful review question

Could another service owner explain who used elevated access, for which task, under whose authority and how it ended? If one of those links is missing, improve the record or process before widening the rollout.

Begin with a controlled application and a realistic support scenario. Prove the approval, activation, extension and revocation paths. The benefit comes from reducing unnecessary standing access while retaining a reliable way to complete legitimate work.

References and further reading

Primary guidance used for the points cited in this paper. Examples, templates and recommended working practices are AIdentX editorial guidance. Sources reviewed September 2026.

NIST SP 800-207: Zero Trust Architecture

https://csrc.nist.gov/pubs/sp/800/207/final

IGAX platform capabilities

https://www.aidentx.com/igax/platform

Put the guidance into practice

Read related articles and explore IGAX platform capabilities at www.aidentx.com/igax/resources.