IGEL Contextual Access™ with Persona Policy

Controlled access to a desktop that is always appropriate for the user's role, advancing the Adaptive Secure Desktop.

Modern work is no longer defined by a device, a single location, or a single desktop.

A clinician may use a shared workstation during a shift change. An administrator may need privileged tools from a managed endpoint. A contractor may require limited access to a specific project.

The challenge for IT and security teams is simple to describe and difficult to solve: how do you deliver the right workspace to the right person, without creating broad access, brittle policies, or operational drag? IGEL's persona-aware control policy in IGEL Contextual Access is designed to address the challenge.

IGEL Contextual Access enables persona-aware control into the IGEL endpoint experience, helping organizations align workspace behavior with who the user is, what role they perform, what groups they belong to, and how they work.

Why persona matters at the endpoint

Identity and access management have advanced significantly. Organizations already rely on platforms such as Microsoft Entra ID, Okta, and Ping to help authenticate users and manage access. But there is often still a gap between identity decisions and what happens at the endpoint.

That gap shows up in everyday scenarios:

- Shared endpoints deliver the same experience to different users
- Contractors receive more access than they need
- Clinical, operational, and administrative users require different workspace behavior on the same device
- IT teams must maintain complex profile structures to reflect real-world user roles
- Security teams want least privilege access, but endpoint execution remains too static

The result is a disconnect between policy intent and endpoint behavior.

IGEL Contextual Access helps close that gap by making user persona an enforceable signal at the endpoint.

Persona-based access policy

IGEL Contextual Access is built around contextual evaluation that helps determine the appropriate access posture, permitted resources, and workspace configuration for each session.

The new persona policy layer, a layer of the IGEL Contextual Access, focuses on the user.

It evaluates signals such as:

Persona Signal	Examples
User identity	Microsoft Entra ID, Okta, Ping
Role	Admin, Clinician, Operator, Contractor
Group membership	Department, security group, business unit, project group
Work profile	Remote worker, shift worker, third party

This allows organizations to define workspace behavior based on real-world user context, not just device assignment.

A clinician can receive a clinical workspace. An administrator can receive privileged tools only when appropriate.
A contractor can receive a restricted workspace. A shift worker can receive the right set of applications and controls on a shared endpoint. The endpoint remains governed. The workspace adapts.

Better security through least-privilege workspace delivery

Rather than treating every user on a device the same way, organizations can shape the workspace by persona. This helps reduce unnecessary access and supports Zero Trust-aligned architecture by making identity and role more meaningful at the endpoint layer.

For security teams, the value is straightforward: fewer broad-access workspaces, tighter control over privileged experiences, and a more governed endpoint model.

Benefit for IT:

IT admins gain a more controlled way to deliver the right workspace without relying only on static device assignment.

Benefit for Users:

Users receive a workspace that matches their role, reducing confusion and limiting exposure to tools or resources they do not need.

Lower operational complexity for IT teams

Without persona-aware policy, IT teams often rely on static device profiles, manual exceptions, or one-off configurations. Those models become hard to manage as roles, locations, and work patterns change.

The persona policy layer helps simplify that model by aligning policy to identity, role, group membership, and work profile. IT can move closer to a centrally governed model where the right experience follows the user, while the device remains managed through the IGEL Universal Management Suite.

Benefit for IT:

IT admins can reduce profile sprawl and manage workspace behavior through a more centralized, identity-aware policy approach.

Benefit for Users:

End users get a more consistent and appropriate experience, even as work patterns, locations, or shared-device usage change.

Industry specific use cases

Workspaces should reflect the person using them. The persona policy layer for IGEL Contextual Access™ helps organizations align endpoint behavior with user identity, role, group membership, and work profile.

Healthcare:

Clinicians, administrators, and shift workers use shared workstations but require different applications, access levels, and controls.

Manufacturing and Operations:

Operators, supervisors, contractors, and administrators use shared endpoints in fast-moving environments where the right workspace matters.

Retail and Frontline:

Employees may move between locations, shifts, and shared devices while requiring role-appropriate access.

Contractor Access:

Third-party users can receive limited, project-specific workspace access instead of broad access to the endpoint experience.

Privileged Access:

Administrators can receive privileged tools only when appropriate.

For more information, schedule a meeting with your trusted IGEL partner or an IGEL expert today.