Intras, Cloud Services

TECHNICAL PRODUCT WHITEPAPER · EXTERNAL EDITION

ICS Governed Property Enablement: Per-Property Identity Control for Multi-Property Hotel Groups

Delegating property-level Microsoft 365 administration with Microsoft Entra ID Administrative Units — without giving away the tenant

Intras Cloud Services · Enterprise Services · Version 1.0 · August 2026 · intrascloudservices.com

1. Executive Summary

Hotel groups rarely operate as one organization. A single Microsoft 365 tenant may cover corporate functions, wholly owned resorts, managed properties, and properties run day-to-day by a third-party management company. The identity platform is shared. The operating reality is not.

This creates a recurring problem for corporate IT. Property-level IT staff and outside management companies need to onboard seasonal staff, reset passwords, and enroll front-desk and back-of-house devices at the speed the property runs. The only tools most tenants offer to grant that access are tenant-wide administrative roles. Granting Helpdesk Administrator or User Administrator at the tenant to a property or an outside operator gives that party reach across every other property in the portfolio. Withholding it pushes every password reset and device enrollment into a corporate queue that cannot match property tempo.

ICS Governed Property Enablement resolves this using Microsoft Entra ID Administrative Units. An Administrative Unit is a container for users, groups, and devices, and Microsoft Entra roles can be assigned with a scope limited to that container, so role permissions apply only when managing members of the unit and do not extend to tenant-wide settings (Microsoft Learn — Administrative units, Microsoft Learn — Assign roles with AU scope). ICS designs the property boundary, builds the naming and group structure that makes it durable, assigns least-privilege roles inside the boundary, tests that the boundary holds, and hands the property a documented operating procedure with a defined escalation path back to corporate.

The outcome for a hotel group is a tenant where a property — or the management company running it — can do its own day-to-day identity work inside a fenced scope, while corporate retains exclusive authority over tenant-level architecture, Conditional Access, and privileged access. This whitepaper describes the reference architecture, the delegation model, the security guardrails, and the ICS delivery method, drawn from ICS Enterprise Services delivery experience with multi-property hospitality tenants.

> **Note on sourcing and content ownership.** This document separates two kinds of content, and the distinction is applied consistently throughout. **Microsoft platform behavior** — what Microsoft Entra ID does, its supported object types, its constraints, and its licensing requirements — carries an inline citation to Microsoft's published documentation and is independently verifiable at the linked source. **ICS methodology** — design decisions, delivery phases, testing approach, operating model, and service structure — carries no external citation, because it is proprietary to ICS. Section 4 makes this split explicit at the section level. Delivery detail is drawn from ICS Enterprise Services engagement experience. Customer names, property names, tenant identifiers, object names, and configuration values are withheld from this document. ICS has not published recovery-time, cost-reduction, or ticket-volume statistics for this offering and does not assert any here.

2. Customer Challenges: Why Hospitality Breaks the Single-Tenant Admin Model

Hospitality has structural characteristics that make tenant-wide delegation particularly risky and particularly tempting.

2.1 Mixed ownership and mixed operators in one tenant

A hotel group's portfolio commonly includes properties it owns and operates, properties it owns and contracts out, and properties operated under management agreements by third parties. All of them may sit in the corporate Microsoft 365 tenant because email domains, brand collaboration, and licensing are centralized there. The tenant therefore contains identities that belong to organizations with no contractual right to see each other's data.

2.2 Property tempo versus corporate change control

A resort that loses a front-desk workstation during check-in does not have hours to wait. Seasonal ramp-up can add and remove large numbers of staff over short windows. Corporate IT change control exists for good reason, but it is not designed to absorb high-volume, low-risk, property-local work.

2.3 The two bad options

Most hotel groups end up choosing between two unacceptable positions:

Option	What property IT gets	What corporate accepts
Grant tenant-wide admin roles	Immediate ability to work	An outside operator can read and modify identities, devices, and groups belonging to every other property
Withhold admin roles	Nothing; every action is a ticket	Slow property response, shadow workarounds, shared accounts, and unmanaged devices

Microsoft is explicit on the underlying mechanic: if a role is assigned to a user who is not scoped to an administrative unit, the scope of the role is the entire tenant (Microsoft Learn — Administrative units).

2.4 Device sprawl and unmanaged joins

Property environments accumulate kiosks, back-office PCs, housekeeping tablets, and engineering laptops. Without a controlled device-join authorization process, devices get joined by whoever happens to have credentials, arrive outside management scope, and never appear in a compliance baseline.

2.5 Hybrid identity debt

Older properties often carry an on-premises Active Directory domain controller inherited from a prior operator or a legacy property management system. Hybrid-joined devices at a property complicate the delegation boundary, because the authoritative object lifecycle sits on-premises rather than in Entra ID.

2.6 Weak audit and offboarding evidence

When delegation is informal, there is no register of who holds which administrative right, no periodic review, and no rollback procedure. During a management-agreement transition — a routine event in hospitality — the group cannot answer with confidence which outside accounts still hold privilege.

2.7 Executive-account exposure

Ownership groups, asset managers, and corporate executives sit in the same tenant as property helpdesk staff. A broadly scoped helpdesk role is a credential-reset path to those accounts.

3. ICS Solution Overview

ICS Governed Property Enablement is a consulting-led engagement that establishes a governed, per-property administrative boundary inside an existing Microsoft 365 tenant and enables property or management-company staff to operate inside it.

The offering has five components.

1. Property boundary design. ICS defines the Administrative Unit scope for the property — which users, devices, and groups belong inside it, with documented inclusion and exclusion criteria and stakeholder approval. Where the property holds sensitive objects, ICS deploys the Administrative Unit with restricted management enabled.

2. Group and naming architecture. Administrative Units are only as reliable as the object structure feeding them. ICS designs a location-and-function group naming convention, builds property device groups, and builds administrative scope groups that carry the delegated role assignments.

3. Least-privilege role delegation. ICS identifies the minimum set of Entra roles the property actually needs for day-to-day work, maps each to an Administrative Unit-scoped assignment rather than a tenant-wide one, and substitutes purpose-built custom roles where a built-in role carries privilege the property should not hold.

4. Device-join governance. ICS defines which accounts and groups may join devices for the property, configures Entra device settings to enforce it, blocks hybrid join where a cloud-native posture is required, and publishes a device-join Standard Operating Procedure for property IT.

5. Co-management operating model. ICS documents the three-tier operating and escalation model — property operations, ICS architecture and governance, corporate approval authority — as a RACI matrix with tiered approval authority and a rollback procedure.

What differentiates the ICS approach

- **Consulting-led, not feature-led.** The Administrative Unit is a Microsoft capability available to any tenant. The value ICS adds is the boundary design, the group architecture that keeps it accurate, the role substitutions that keep it least-privilege, and the governance that keeps it true over time.
- **Tested boundaries, not assumed boundaries.** ICS executes test scenarios per delegated role to confirm that property staff can manage objects inside the unit and cannot reach objects outside it, and documents the evidence.
- **Hospitality operating reality.** The model is built for the management-company and franchise structures that define the industry, not adapted from a single-entity corporate template.
- **Reversibility by design.** Delegation without a documented revocation path is an unmanaged risk. ICS delivers an emergency access shutdown procedure covering Administrative Unit

disablement and role revocation.

4. Architecture and Technical Design

How to read this section. Section 4 is deliberately divided. Part 1 describes Microsoft Entra ID platform behavior — every statement is cited to Microsoft's own documentation and applies to any tenant, regardless of who performs the work. Part 2 describes the ICS design decisions built on top of that platform behavior. These are ICS methodology, not Microsoft defaults, and are the part of this document that reflects ICS delivery experience.

Part 1 — Microsoft Entra ID platform behavior

Every statement in Part 1 is documented by Microsoft and independently verifiable at the linked sources.

4.1 What an Administrative Unit is and is not

An Administrative Unit is a Microsoft Entra resource that acts as a container for other Entra resources. It can contain **only users, groups, and devices** — no other object types (Microsoft Learn — Administrative units).

Two documented behaviors drive the entire design and are the most common source of misconfiguration:

- **Group containment is not member containment.** Adding a group to an Administrative Unit brings the group object into scope — an administrator scoped to the unit can manage the group's name and membership. It does **not** bring the group's members into scope. A User Administrator scoped to a unit containing a group cannot manage those members' user properties, cannot manage their authentication methods, and cannot reset their passwords unless those users are added directly as members of the Administrative Unit (Microsoft Learn — Administrative units).
- **Unit scope is not tenant scope.** An Administrative Unit-scoped role assignment applies only when managing members of the unit. It does not grant permission over tenant-wide settings — a Groups Administrator scoped to a unit cannot manage tenant-level group expiration or naming policies — and it does not grant permission to manage the Administrative Unit object itself (Microsoft Learn — Assign roles with AU scope).

A third behavior explains why the delegation problem exists at all: if a role is assigned to a user who is not scoped to an Administrative Unit, the scope of that role is the entire tenant (Microsoft Learn — Administrative units).

4.2 Restricted management Administrative Units — platform behavior

In a restricted management Administrative Unit, only administrators with an explicit assignment at that unit's scope can change the Entra properties of the contained objects. A Global Administrator cannot modify those objects unless the Global Administrator explicitly assigns themselves a role scoped to that unit, and that self-assignment is an auditable event (Microsoft Learn — Restricted management administrative units).

Supported object types differ from a regular Administrative Unit:

Object type	Regular AU	Restricted management AU
Users	Yes	Yes
Devices	Yes	Yes
Security groups	Yes	Yes
Microsoft 365 groups	Yes	**No**
Mail-enabled security groups	Yes	**No**
Distribution groups	Yes	**No**

Source: Microsoft Learn — Restricted management administrative units

Within a restricted management unit, operations that directly modify Entra properties of contained objects are blocked for administrators without an explicit assignment at that scope — including modifying properties, deleting the object, updating a password, and modifying group owners or members. Reading standard properties remains allowed. Several operations in adjacent services are **not** blocked: modifying Exchange mailbox and email settings, applying Intune policy to a contained device, adding or removing a group as a SharePoint site owner, adding contained objects to other Entra groups, and assigning licenses or updating usage location (Microsoft Learn — Restricted management administrative units).

Microsoft warns directly that placing objects in a restricted management Administrative Unit severely restricts who can make changes and can cause existing workflows to break (Microsoft Learn — Restricted management administrative units).

4.3 Platform limits

Constraint	Value
Administrative Units per tenant	No specific limit
Restricted management AUs per tenant	Maximum 100
AU memberships per Entra resource	Maximum 30

Constraint	Value
Dynamic groups and dynamic AUs, combined	Maximum 15,000

Source: Microsoft Learn — Directory service limits and restrictions

Creating Administrative Units and assigning roles over them requires the Privileged Role Administrator role (Microsoft Learn — Manage administrative units).

Part 2 — ICS design decisions

The following are ICS design positions and methodology. They are choices, not platform requirements, and they are what ICS brings to an engagement beyond the documented capability described in Part 1.

4.4 Reference architecture for a single property

```
Corporate Microsoft 365 Tenant
│
├── Tenant-level controls  [CORPORATE + ICS ONLY]
│     Conditional Access framework
│     Privileged Identity Management (PIM) configuration
│     Cross-tenant / third-party integration governance
│     Tenant device registration settings
│     Group naming, expiration, and lifecycle policy
│
├── Administrative Unit: <PROPERTY>            (restricted management where required)
│     ├── Users:   property staff accounts (added DIRECTLY — see 4.1)
│     ├── Devices: property-owned Entra-joined devices
│     └── Groups:  property security, device, and admin scope groups
│
├── AU-scoped role assignments  →  PROPERTY / MANAGEMENT COMPANY IT
│     Custom "<Property> User Manager" role   (license assignment removed)
│     Authentication Administrator            (AU scope)
│     Groups Administrator                    (AU scope)
│     Device-related roles as required        (AU scope)
│     Delivered PIM-eligible where licensing supports it
│
├── Group-scoped Conditional Access
│     Property policies target property groups, not the AU object
│
└── Intune scope tag: <PROPERTY>-Devices
      Controls which Intune objects property admins can see
```

ICS position on Conditional Access targeting. Conditional Access policies are targeted at groups rather than at the Administrative Unit. The Administrative Unit governs who may administer objects; groups govern which policies apply to them. Keeping these separate prevents a delegation change from silently altering security policy coverage. This is an ICS design rule, not a platform constraint.

4.5 Group and naming architecture

Administrative Units do not solve object organization; they consume it. ICS designs and secures approval for the group architecture before any Administrative Unit work begins. The convention uses a location-and-function pattern with a client-specific prefix on every group and distinct type markers for security groups, Microsoft 365 groups, distribution lists, mail-enabled security groups, device groups, administrative scope groups, license groups, and policy groups. Location codes identify each property, a dedicated global code identifies portfolio-wide groups, and department codes cover hospitality-specific functions.

Three group classes carry the architecture:

Group class	Purpose	Membership
Property device groups	Target Conditional Access, compliance, and configuration to property-owned devices	Dynamic where a reliable device attribute exists; static otherwise
Property user groups	Target Conditional Access and licensing to property staff	Static or dynamic by property attribute
Administrative scope groups	Hold the delegated administrators who receive AU-scoped roles	Static, tightly controlled, reviewed on a defined cadence

4.6 ICS position on restricted management

Restricted management is applied selectively rather than by default. ICS enables it where a property's objects must be protected from broadly scoped administrators elsewhere in the tenant, and where ownership, executive, or asset-management accounts share the tenant with property helpdesk staff.

Because Microsoft states that restricted management can break existing workflows, ICS treats workflow-impact analysis as a required design step. Because Microsoft 365 groups, mail-enabled security groups, and distribution groups cannot be members of a restricted management unit, the group architecture in 4.5 is designed so that collaboration objects and delegation objects are distinct — a property's security and device groups can be protected without stranding its mail and collaboration groups.

The 100-unit restricted management ceiling is treated as a portfolio planning constraint: restricted management is reserved for properties and object sets that require it rather than applied uniformly.

4.7 Cloud-native device posture

ICS designs the property boundary to a cloud-native target posture: no on-premises Active Directory dependency for property objects, no hybrid join, no directory synchronization for in-scope objects, and no legacy authentication path. Where an assessment confirms that posture already exists, ICS enforces it going forward — documenting the Entra-only device requirement,

configuring Entra device settings to enforce the approved join policy, blocking hybrid join for the property device group, and validating by test that only cloud-native Entra join succeeds. Where on-premises dependency is present, ICS documents it as a remediation requirement rather than designing the boundary around it.

For hospitality this is a material design decision. A cloud-native property has no domain controller to maintain, patch, or lose in a flood or power event, no site-to-site dependency for authentication, and no on-premises object lifecycle competing with the Administrative Unit boundary. It also removes an entire class of legacy authentication exposure from the property network.

5. Features and Capabilities

5.1 Base service

Capability	What ICS delivers
Tenant and property structure assessment	Assessment of current Entra Administrative Unit capability against property requirements; documented capability gaps and licensing dependencies; mapping of tenant structure to identify where the property boundary fits
Cloud-native confirmation	Audit confirming absence of on-premises AD dependency for property objects; documented findings and remediation requirements
AU scope definition	Complete definition of property users, devices, and groups in scope, with inclusion and exclusion criteria, rationale, and stakeholder approval
AU build	Creation of the Administrative Unit with restricted management enabled where required; documented configuration; validation that restricted management is enforced
AU population and validation	Population per the approved scope; validation that object containment matches the design; identification of objects that cannot be added due to platform restrictions
Group architecture	Location-and-function naming convention; property device groups with dynamic membership rules where applicable; administrative scope groups; documented purpose, membership rule, and owner per group
Role requirement analysis	Minimum role set required for property day-to-day operations, defined jointly with the property or management company under least-privilege principles, with operational justification per role

Capability	What ICS delivers
AU-scoped role assignment	Each role mapped to an AU-scoped assignment rather than tenant-wide, configured through PIM where applicable, with each assignment individually validated
Boundary enforcement testing	Test scenarios per delegated role confirming property staff can manage inside the unit and cannot access or modify objects outside it; documented results
Device-join authorization	Defined authorized joiner accounts and groups; Entra device settings configured to enforce the policy; hybrid join blocked where a cloud-native posture is required; end-to-end join test with documented results
Device registration workflow	Request submission, review, approval criteria, registration steps, and post-registration validation, with SLA targets per step
Property device-join SOP	Standard Operating Procedure for property and management-company IT: prerequisites, step-by-step instructions, troubleshooting, and escalation to ICS
Role assignment register	Register of every AU-scoped role assigned, with assignee, business justification, and approval date — the baseline for periodic access review
Co-management operating model	Documented responsibilities for property operations, ICS, and corporate; three-tier escalation path; tiered approval authority; RACI matrix published under version control
Rollback and emergency controls	Documented step-by-step Administrative Unit disablement and role-revocation procedure

5.2 Optional add-ons

Add-on	Description
Portfolio rollout	Extension of the validated single-property pattern across additional properties, including per-property scope definition, build, and boundary testing
Conditional Access framework	Design and deployment of the property and portfolio Conditional Access policy set, current-state and target-state documentation, and change-management handoff

Add-on	Description
Privileged Identity Management deployment	PIM configuration for eligible role activation, approval workflow, and activation review
Third-party integration governance	Governance policy and review standard for property-level SaaS integrations, covering the hospitality application estate — property management systems, central reservation systems, catering and event platforms, guest reservation platforms, and spa and activity systems — with least-privilege review of each integration's tenant permissions
Intune scope tag delegation	Design and deployment of property Intune scope tags so property administrators see only Intune objects relevant to their property. Roles determine what access administrators have; scope tags determine which objects they can see (Microsoft Learn — Intune scope tags)
Management-agreement transition support	Delegation revocation, re-delegation, and evidence package for a change of property operator

6. Security, Compliance, and Governance

6.1 Least privilege as an engineering decision, not a slogan

A consequential ICS design decision is to replace a built-in role with a purpose-built custom role where the built-in role is too broad. The built-in User Administrator role carries license-assignment capability. Where a property's delegated staff has no business need — and no commercial authority — to assign licenses that the hotel group pays for, ICS defines a custom property user-management role that omits that permission and assigns it at the Administrative Unit scope instead.

This is representative of the pattern ICS applies throughout: for every capability the property needs, identify the narrowest role that provides it, and where no built-in role is narrow enough, build a custom one. Any custom role can be assigned with Administrative Unit scope provided its permissions include at least one permission relevant to users, groups, or devices (Microsoft Learn — Assign roles with AU scope).

6.2 Roles available for property delegation

Microsoft supports Administrative Unit scope for a defined set of built-in roles, including Authentication Administrator, Groups Administrator, Helpdesk Administrator, User Administrator, Attribute Assignment Administrator and Reader, and others, plus any qualifying custom role

(Microsoft Learn — Assign roles with AU scope). ICS assigns from this set only what the property's documented operational needs require.

6.3 Zero Trust alignment

Zero Trust principle	How the property model applies it
Verify explicitly	Property administration operates under the tenant Conditional Access framework; privileged activation runs through PIM where licensing supports it
Use least-privilege access	AU-scoped assignments replace tenant-wide roles; custom roles strip capabilities the property does not need; PIM eligibility replaces standing privilege
Assume breach	Restricted management limits what a compromised broadly scoped account elsewhere in the tenant can reach; the AU boundary limits lateral reach from a compromised property administrator; a documented disable-and-revoke procedure limits dwell time

6.4 Segregation of duties across the portfolio

The Administrative Unit boundary produces a defensible segregation-of-duties position that a shared tenant otherwise cannot support. A management company operating one property in a portfolio holds administrative rights over that property's objects and no others, and that limitation is enforced by the platform rather than by policy language. Where restricted management is enabled, corporate can additionally demonstrate that even tenant-level Global Administrators cannot silently modify protected property objects without an auditable self-assignment (Microsoft Learn — Restricted management administrative units).

6.5 Audit evidence

The engagement produces a defined evidence set: the approved scope document, the AU configuration record, the boundary enforcement test results, the role assignment register with per-assignment business justification and approval date, the device-join SOP, the device registration workflow with SLA targets, and the RACI matrix under version control. This is the material an internal audit function, a cyber insurance underwriter, or a brand compliance review will ask for.

6.6 Governance boundaries ICS states explicitly

ICS documents what it does **not** commit to, so the operating model is not read as a broader agreement than it is:

- ICS retains ownership of tenant-level architecture decisions — Conditional Access framework, PIM configuration, security group design, Administrative Unit structure, and integration

governance — under a defined change-management process.

- Corporate remains the approval authority for tenant-level changes. ICS does not perform tenant administration or configuration changes without authorization from the designated corporate approver or an approved backup approver.
- The property or management company may act directly inside its Administrative Unit for scoped user and device work.
- ICS does not provide active monitoring, detection, or SLA-bound containment under this offering unless separately contracted. Where a security event is reported, ICS assesses and recommends containment, and executes containment after authorization.
- Emergency access and kill-switch authority is defined in the risk-controls and rollback deliverable, not implied by the operating model.

6.7 Licensing dependencies

Requirement	License
Each Administrative Unit administrator assigned directory roles over the unit's scope	Microsoft Entra ID P1
Each Administrative Unit member	Microsoft Entra ID Free
Creating Administrative Units	Microsoft Entra ID Free
Each Administrative Unit member where dynamic membership rules are used for the unit	Microsoft Entra ID P1
Each user with a custom role assignment	Microsoft Entra ID P1
PIM eligibility, time-bound assignment, and activation controls	Microsoft Entra ID P2 with Privileged Identity Management

Sources: Microsoft Learn — Microsoft Entra ID licensing, Microsoft Learn — Assign roles with AU scope

Creating and administering Administrative Unit role assignments requires the Privileged Role Administrator role (Microsoft Learn — Manage administrative units).

7. Implementation Approach and Methodology

ICS delivers Governed Property Enablement in six phases.

Phase 1 — Assess

Assess current Entra Administrative Unit capability against property requirements. Document capability gaps and licensing dependencies. Map the existing tenant structure to identify where the property boundary fits. Audit the property environment to confirm or refute on-premises Active Directory dependency.

Deliverables: capability and gap assessment; cloud-native confirmation with remediation list.

Phase 2 — Design

Define the Administrative Unit scope — users, devices, and groups — with inclusion and exclusion criteria and documented rationale. Design or validate the group naming convention and group class structure. Identify the minimum role set the property requires, with operational justification per role, and determine where a custom role must replace a built-in role. Determine whether restricted management is required and analyze workflow impact if it is.

Deliverables: approved AU scope document; group architecture and naming standard; role requirement matrix with AU-scoped assignment mapping.

Gate: ICS and corporate stakeholder approval of scope and role model before any build.

Phase 3 — Build

Create the Administrative Unit with restricted management where required. Build property device groups and administrative scope groups. Create the custom roles. Populate the unit per the approved scope. Assign the approved roles at Administrative Unit scope, through PIM where applicable, validating each assignment individually.

Deliverables: AU configuration record; group register with purpose, membership rule, and owner; role assignment register.

Phase 4 — Enforce Device Governance

Define which accounts and groups may join devices for the property. Configure Entra device settings to enforce the join policy. Block hybrid join where a cloud-native posture is required. Design the device registration approval workflow with SLA targets per step.

Deliverables: device-join authorization definition; device settings configuration record; device registration approval workflow.

Phase 5 — Validate

Validate AU membership against the scope definition and remediate any missing or incorrectly included objects. Execute boundary enforcement tests per delegated role, confirming that

property staff can manage objects inside the unit and cannot access or modify objects outside it. Execute an end-to-end device join test in the property scope. Confirm hybrid join is blocked.

Deliverables: AU membership validation report; per-role boundary test results with evidence; device join test results.

Gate: No delegation is released to the property until boundary tests pass and are documented.

Phase 6 — Operationalize and Hand Off

Publish the device-join SOP for property IT. Publish the co-management operating model, three-tier escalation path, tiered approval authority model, and RACI matrix under version control. Document the emergency Administrative Unit disablement and role revocation procedure. Establish the access review cadence against the role assignment register.

Deliverables: property device-join SOP; co-management operating model; RACI matrix; emergency access shutdown runbook.

Timeline and prerequisites

A single-property engagement is typically delivered over a small number of weeks, driven less by technical build effort than by three dependencies: stakeholder availability to approve scope and role model, property or management-company participation in defining operational role needs, and completion of any remediation identified in Phase 1.

Delivery risk ICS flags at kickoff. In ICS delivery experience, the largest schedule risk on these engagements is not technical. It was the availability of the third-party management company to participate in scope and role definition. Governed Property Enablement requires an accountable, named operational contact at the property or management company. ICS requires that contact be designated before Phase 2 begins and escalates when participation lapses. Corporate sponsors should treat this as a condition of delivery rather than a detail.

8. Operations, Support, and Managed Services

Once the boundary is live, three functions must persist. ICS defines them explicitly and delivers them under separate contract where the group elects managed support.

Function	Description
Property intake	Property and management-company requests route through a defined service desk queue under a property tag, rather than ad hoc email to individual engineers
Access review	Periodic review of the role assignment register against current property staffing and current business justification, with revocation of assignments no longer justified

Function	Description
Governance review	Trigger-based review of the delegation model when the property adds systems, changes operator, changes staffing model, or experiences a security event
Change management	Tenant-level changes — Conditional Access, PIM, group architecture, AU structure — proceed only under the documented change process with corporate approval
Escalation	Three-tier path: property operations, then ICS architecture and governance, then corporate decision authority, with defined trigger criteria per tier
Rollback	Documented Administrative Unit disablement and role revocation procedure, exercised rather than assumed

Scope boundary. Under Governed Property Enablement, ICS does not provide active monitoring, detection, or SLA-bound containment. Corporate holds accountability for authorizing incident response. Where the group requires continuous monitoring and response, that is delivered under a separate ICS managed security engagement.

9. Customer Outcomes and Benefits

ICS states outcomes as control and capability changes that can be verified in the tenant and in the delivered evidence set. ICS does not publish ticket-reduction, cost-reduction, or time-to-resolution statistics for this offering and does not assert any here.

Business concern	What changes
Cross-property exposure	Property and management-company administrative rights are bounded to that property's objects by platform enforcement, not by policy language. Where restricted management is enabled, even tenant-level Global Administrators cannot modify protected property objects without an auditable self-assignment
Property responsiveness	Property staff perform their own password resets, user lifecycle work, group membership changes, and device enrollments inside the boundary, at property tempo
Corporate control	Corporate and ICS retain exclusive authority over Conditional Access, PIM, group architecture, AU structure, and integration governance
Executive account protection	Corporate and ownership accounts sit outside the property boundary and are not reachable by property-delegated roles
Device governance	Devices enter the tenant through a defined authorization and approval workflow with SLA targets, not through whoever holds credentials

Business concern	What changes
Legacy infrastructure	A cloud-native property posture removes on-premises domain controller dependency, and the associated maintenance, physical risk, and legacy authentication exposure, from the property
Audit and insurance readiness	The engagement produces a scope document, configuration record, boundary test evidence, role assignment register with justifications, SOP, workflow, and RACI — the artifacts audit and underwriting request
Operator transitions	A documented role register and rollback procedure make delegation revocation a defined procedure at management-agreement change, rather than a discovery exercise
Scalability	A validated single-property pattern is repeatable across the portfolio without re-litigating the design

10. Use Cases and Industry Scenarios

10.1 Luxury resort operated by a third-party management company

A hotel group owns a mountain resort but contracts day-to-day operations to a management company. The management company's IT staff need to onboard seasonal staff at ramp-up, reset passwords, and enroll front-desk and back-of-house devices. They must not be able to see or modify identities at any other property in the portfolio, and must not be able to assign licenses the group pays for.

ICS deploys a restricted management Administrative Unit containing the resort's users, devices, and groups; assigns the management company a custom property user-management role at that scope with license assignment removed, plus authentication and group administration at the same scope; configures device-join authorization limited to named management-company and ICS accounts; and publishes the device-join SOP and escalation path. This is the most common Governed Property Enablement scenario in hospitality.

10.2 Multi-property portfolio standardizing delegation

A group with a dozen properties has accumulated inconsistent delegation — some properties hold tenant-wide helpdesk roles, others hold nothing, and no one can produce a list of who holds what.

ICS establishes the group naming and structure standard, builds one Administrative Unit per property, migrates each property's delegation to AU-scoped assignments, retires the tenant-wide grants, and produces a single portfolio-wide role assignment register. Because Entra imposes no specific limit on the number of Administrative Units per tenant, the one-unit-per-property model scales with the portfolio (Microsoft Learn — Directory service limits and restrictions).

10.3 New property opening

A group is opening a new resort with a construction-phase IT team and a permanent operations team taking over at handover.

ICS builds the property's Administrative Unit, group structure, and device-join governance before opening, delegates temporary scoped access to the pre-opening team through PIM-eligible assignments with defined end dates, and transitions delegation to the permanent team at handover. The role assignment register documents both states.

10.4 Property leaving the portfolio

A management agreement ends, or a property is sold.

ICS executes the documented revocation procedure — disable or reconfigure the Administrative Unit, revoke AU-scoped role assignments, and produce a closure evidence package. Because every delegated assignment is recorded in the register with a justification and approval date, revocation is a checklist rather than an investigation.

10.5 Executive and ownership account protection

A group's tenant contains ownership principals, asset managers, and corporate executives alongside property helpdesk staff.

ICS places those accounts and their devices in a restricted management Administrative Unit so that broadly scoped helpdesk roles elsewhere in the tenant cannot reset their credentials or reach their device recovery information. Microsoft identifies protecting C-level executive accounts and their devices from Helpdesk Administrators as a primary use of restricted management Administrative Units (Microsoft Learn — Restricted management administrative units).

11. Prerequisites and Dependencies

Platform prerequisites

- An existing Microsoft Entra ID tenant with the group's properties represented in it.
- Microsoft Entra ID P1 for each delegated property administrator holding AU-scoped directory roles, and for each user holding a custom role assignment. P2 with Privileged Identity Management where PIM-eligible assignment, time-bound assignment, or activation approval is required (Microsoft Learn — Microsoft Entra ID licensing).
- Privileged Role Administrator access for Administrative Unit creation and role assignment (Microsoft Learn — Manage administrative units).
- Where a cloud-native posture is required: no on-premises Active Directory dependency for property objects, or an agreed remediation path.

- Microsoft Intune where device compliance, configuration, or scope tag delegation is in scope.

Organizational prerequisites

- A named corporate approver for tenant-level changes, and a named backup approver.
- A named, accountable operational contact at the property or management company, designated before design begins.
- Documented property staffing and role needs from the property or management company.
- Executive sponsorship for the governance model and the approval tiers it defines.

Dependencies and constraints to plan for

- **Group containment does not confer member management.** Users requiring property-level management must be added directly to the Administrative Unit, not merely be members of a group in it (Microsoft Learn — Administrative units).
- **Restricted management units exclude Microsoft 365, mail-enabled security, and distribution groups**, and may break existing workflows (Microsoft Learn — Restricted management administrative units).
- **Restricted management does not extend to every adjacent service.** Exchange mailbox settings, Intune policy application, SharePoint site ownership changes, group additions, and license assignment remain permitted for administrators outside the unit's scope (Microsoft Learn — Restricted management administrative units).
- **Platform ceilings.** Maximum 100 restricted management Administrative Units per tenant; maximum 30 Administrative Unit memberships per Entra resource; maximum 15,000 dynamic groups and dynamic Administrative Units combined (Microsoft Learn — Directory service limits and restrictions).
- **Third-party property applications.** Property management systems, central reservation systems, catering and events platforms, guest reservation platforms, and spa and activity systems vary in federation capability. ICS documents applications whose single sign-on support is unconfirmed as pending vendor confirmation rather than representing them as federation-capable.

12. Service Packages and Options

Governed Property Enablement is delivered as a fixed-fee engagement scoped to the customer's portfolio, under ICS PMO delivery standards. Scope tiers range from a single property to a portfolio-wide delegation standard, with optional modules covering Conditional Access framework design, Privileged Identity Management deployment, third-party integration governance, Microsoft Intune scope tag delegation, and multi-property rollout.

Ongoing access review, governance review, and new-property intake are delivered under a separate managed services agreement.

Package composition and commercial terms are provided during scoping. Contact ICS for a scoped proposal.

13. Summary and Next Steps

Hotel groups do not need to choose between property responsiveness and tenant control. That choice is an artifact of tenant-wide administrative roles, not a property of the platform. Microsoft Entra ID Administrative Units allow role permissions to be scoped to a defined container of users, groups, and devices, so a property — or the management company operating it — can do its own identity and device work inside a fenced boundary while corporate retains exclusive authority over everything above it.

What makes that boundary hold is not the container. It is the group architecture beneath it, the least-privilege role design inside it, the tested proof that it cannot be crossed, the register of who holds what and why, and the documented procedure for taking it away. That is the work ICS delivers.

Next steps

1. **Engage ICS for a Governed Property Enablement Readiness Assessment.** ICS assesses your tenant's Administrative Unit capability, maps your property structure, identifies on-premises dependencies and licensing gaps, and produces a prioritized delegation roadmap.
2. **Schedule a Solution Design Workshop.** Define the property boundary, the group architecture, and the least-privilege role model with your corporate IT, security, and property stakeholders in one session.
3. **Request a Governed Property Enablement proposal** for a pilot property, with an option to extend the validated pattern across the portfolio.

Contact ICS Enterprise Services to begin.

Appendix A — Sources

Microsoft platform documentation:

- Administrative units in Microsoft Entra ID
- Restricted management administrative units in Microsoft Entra ID
- Assign Microsoft Entra roles with administrative unit scope
- Manage administrative units in Microsoft Entra ID

- Microsoft Entra service limits and restrictions
- Microsoft Entra ID licensing
- Microsoft Entra built-in roles reference
- Use role-based access control and scope tags for distributed IT in Intune

---