



AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Business Phone System Admin Permissions: Routing Checklist

Get a business phone number with a simple auto attendant menu from Auto Attendant. A caller picks who they need and the call rings that person's own mobile, so nobody on your team has to publish a personal number.

Published by Auto Attendant · 2026-10-16 · business phone system admin permissions · call routing permissions · phone account ownership · auto attendant · phone system administrator roles · number porting authorization · business phone security · account recovery

Original article: <https://autoattendant.io/articles/business-phone-call-routing-permissions>



In this article

1. [Executive Summary](#)
 2. [Introduction and Background](#)
 3. [Define the Three Layers of Phone Control](#)
 4. [Identify Who Can Change Routing and Account Ownership](#)
 5. [Match Each Security Control to the Action It Protects](#)
 6. [Separate Audit Logs from Independent Change Alerts](#)
 7. [Run a Reversible Owner-Approved Acceptance Test](#)
 8. [Maintain Recovery, Offboarding and an Unexpected-Change Procedure](#)
 9. [Data Analysis and Evidence](#)
 10. [Implications and Future Directions](#)
 11. [Frequently Asked Questions \(FAQs\)](#)
 12. [Conclusion](#)
-

Executive Summary

Business phone system admin permissions determine who can alter the path between a public number and the people answering it. Receiving calls should be treated as a separate responsibility from administering that path. Provider implementations differ: **Microsoft Teams** can authorize specific voice-application changes without assigning an administrative role, while **Quo** documents phone-number access separately from workspace roles. A business should therefore request an action-by-action demonstration rather than rely on labels such as user, manager, or administrator. (learn.microsoft.com) (learn.quo.com)

The practical assessment has **three layers**: the public-number provider, the receiving mobile accounts and devices, and the email and authentication channels used to administer or recover them. **Verizon Business** distinguishes SIM Protection from Number Lock and states that neither is enabled by default on the documented accounts. **T-Mobile** separately limits the applicability of its SIM Protection feature. These are mobile-service controls, not evidence that a separate inbound menu cannot be edited. Prioritize strong authentication for administrators, following **CISA** guidance, but ask what the particular phone provider actually supports. (www.verizon.com) (www.t-mobile.com) (www.cisa.gov)

An audit trail and an independent alert answer different questions. **Dialpad** documents administrator changelog exports with an emailed download link. **RingCentral** documents an Audit Trail application programming interface (API) in beta, with limits of up to **180 days** and **10,000 records** per account. Its separate Labs notification app lists forwarding changes, but is a community project with stated support limitations. These examples justify asking for a supported demonstration, not assuming every plan includes the same monitoring or building a custom integration. (help.dialpad.com) (developers.ringcentral.com) (www.ringcentral.com)

Before acceptance, obtain written answers for who can change routes, voicemail recipients, recovery details and transfer credentials; which changes create logs or independent alerts; and how an authorized owner regains access. Then approve a harmless, reversible demonstration on a test number or temporary route. Record the outcome, undo the change, and test external calls again. Maintain a recovery path that does not

depend entirely on the affected number or mailbox. Google's recovery guidance illustrates the value of a different recovery email and backup verification codes, without establishing what any phone provider offers. An unverified required control should remain **unknown**, and should prevent acceptance until demonstrated or resolved through another provider. (support.google.com)

Introduction and Background

A small firm's public phone number may lead to a menu, several staff mobiles and a voicemail destination. The purchasing question is not simply whether the account has a password. It is whether the owner can identify every person permitted to change those destinations, observe a consequential change and recover administration through a verified process. Provider documentation shows why precision matters: **Zoom Phone** describes permissions for specified auto receptionists, including voicemail-inbox access and forwarded-voicemail email destinations. That is a more useful unit of analysis than the broad word access. (support.zoom.com)

This report addresses U.S. owners of trades and professional firms reviewing a business number that rings existing staff mobiles. It treats **call recipients**, **routing administrators**, **account owners**, and **recovery contacts** as distinct responsibilities to map. The names and separation available in a product must come from that product's documentation. For example, **Google Voice** describes a ring group management role, while **Nextiva NEXT** distinguishes its administrator settings from Agent and Supervisor access. Those examples do not establish a universal permissions hierarchy. (knowledge.workspace.google.com) (help.nextiva.com)

The evidence was reviewed for publication on **October 16, 2026**. The report compares documented controls rather than measuring provider reliability or predicting losses. Its tables are a buyer's acceptance framework, not a ranking. It does not infer legal ownership from account possession, prescribe a number-transfer deadline, or assume a wireless lock applies to a hosted business number. Where documentation leaves a capability unresolved, the worksheet records an unknown instead of a negative feature claim.

The publishing site's position is that of an inbound-menu provider serving businesses whose staff answer on existing mobiles. That position makes the distinction between receiving calls and managing the public number especially relevant. It does not supply evidence about the publisher's authentication, logging, alerting or recovery capabilities. Those require the same written confirmation requested of any other provider. The starting point for administrator authentication is the strongest available method, as recommended by CISA, followed by verification of the chosen service's actual implementation. (www.cisa.gov)

Define the Three Layers of Phone Control

Public-number administration is the first layer. List the account that holds the customer-facing number and the supported interface for editing its greeting, menu, business hours, destinations and voicemail recipients. Treat the ability to invite another administrator or modify recovery information as a separate action. Microsoft's voice applications policies illustrate that configuration changes can be enabled through explicit policy rather than a general assumption that an authorized user can change everything. (learn.microsoft.com)

Receiving mobile control is the second layer. Record who controls the mobile account and who holds the device. A route may point to the expected number while that mobile account has its own unresolved access problem. Conversely, protecting the mobile subscription does not demonstrate a restriction on editing the public menu. Verizon's documented SIM Protection concerns transactions requiring a new physical SIM or electronic SIM (eSIM); its Number Lock addresses moving the mobile number to another carrier. Assess those actions separately from hosted routing edits. (www.verizon.com)

Recovery and authentication channels form the third layer. Identify the mailbox, recovery address, authentication device and backup method needed to administer each account. Google recommends a recovery email different from the email used to sign in. That distinction is useful, but two addresses can still depend on the same device or administrator. The recommended dependency map therefore asks whether losing the business number also removes access to the email or verification method needed to restore it. (support.google.com)

Table 1 maps actions to the layer where evidence is needed. The final column states what the cited example establishes and what still requires testing.

Action	Layer and authorized actor to record	Documented example and coverage boundary
Edit menu or business-hours routing	Public provider; named routing administrator	Teams requires the applicable authorization and voice applications policy. Receiving calls alone is not the documented delegated workflow. (learn.microsoft.com)
Change voicemail access or forwarded recipient	Public provider; administrator for the specified object	Zoom documents voicemail-inbox users and forwarded-voicemail recipients within auto-receptionist privileges. Confirm the target scope. (support.zoom.com)
Change a SIM or eSIM	Destination mobile; carrier-authorized actor	AT&T's documented Wireless Account Lock includes SIM and eSIM changes. Confirm applicability to the actual account and supported portal. (www.att.com)
Move a mobile number to another carrier	Destination mobile; holder of transfer authority	T-Mobile documents Port Out Protection added to each line. This does not establish a lock on a separate hosted menu. (www.t-mobile.com)
Recover administrative email	Recovery channel; authorized mailbox owner or administrator	Google describes backup codes for loss of the usual phone-based verification method. Verify the actual email service and policy. (support.google.com)

The matrix prevents a control from being credited to the wrong layer. Extend its private copy with **provider citation, enabled status, independent alert, recovery contact and unknowns**. Record who verified each answer and where the supporting response is securely stored. The public worksheet should contain role names and evidence references, not credentials or customer data.

Identify Who Can Change Routing and Account Ownership

Who can change business call routing? The answer is the set of identities authorized for that specific routing object and action. It can include delegated staff as well as broad administrators. Teams explicitly permits authorized users without an administrative role, while its voice applications policies determine

permitted configuration changes. Ask the provider to show both the assignment and the operative policy, rather than showing only a staff list. (learn.microsoft.com)

Phone system administrator roles also differ in scope. Zoom states that its Phone roles do not grant group-level or account-level phone policy access, which instead requires account-level role management. Google requires a Voice license and phone number for a ring group manager to access the Voice web app. These are platform-specific prerequisites, not reasons to assume every person receiving a forwarded call needs an administrator account or a software seat. (support.zoom.com) (knowledge.workspace.google.com)

Table 2 compares documented permission boundaries. It includes the publisher as an option requiring the same acceptance evidence; unknown means unverified in this report, not confirmed absence.

Provider or product	Documented control model	Acceptance question or unresolved boundary
Microsoft Teams	Authorized users can manage selected voice applications without an administrative role. (learn.microsoft.com)	Which policy permits the exact routing edit, and what licensing does it require?
Zoom Phone	Auto Receptionist Admin privileges include voicemail-inbox access and forwarded-voicemail recipients for target objects. (support.zoom.com)	Can the proposed administrator affect another receptionist or account policy?
Google Voice	A ring group management role delegates selected group management; ring group editing is documented for Standard and Premier subscriptions. (knowledge.workspace.google.com)	Which group and member changes are allowed, and who assigns managers?
Quo	Phone-number access is assigned separately from workspace roles. (learn.quo.com)	Which role may change the public number's routing, voicemail and administrators?
Nextiva NEXT	Agents and Supervisors lack the documented Administrator Settings access without Administrator rights. (help.nextiva.com)	Does the purchased product use this model, and which user-level forwarding settings remain available?
autoattendant.io (publisher)	Inbound-menu provider under review; administration must be assessed separately from receiving calls.	Unknown in this report: role scope, MFA, logs, change alerts, recovery process and transfer protection. Obtain current written answers and a supported demonstration.

The table should narrow demonstrations, not produce a feature score. In **Ooma Office**, for example, the End User Portal lets users update preferences for their own extension. That supports a question about personal-extension control; it does not prove authority over company-wide routing or ownership recovery. A recipient's own forwarding or voicemail preferences may deserve review even when company administration is restricted. (www.ooma.com)

Business phone account ownership should be recorded operationally: who is recognized by the provider, which business account is involved, and how authority is transferred. Twilio's documented self-service ownership-change methods require Organizations and corporate domains for the current and new owners; it

also says a subaccount cannot be assigned an owner. These constraints illustrate why an owner's ability to regain control must be confirmed for the actual account structure. They do not establish anyone's legal entitlement to a number. (help.twilio.com)

Match Each Security Control to the Action It Protects

Passwords and multifactor authentication (MFA) protect account sign-in under the provider's implementation. CISA recommends prioritizing administrative and sensitive-data accounts and aiming for phishing-resistant MFA. Ask which methods the phone and email providers support, whether they can be required for privileged users, and how a replacement authenticator is approved. Do not mark MFA enabled because a vendor supports it somewhere in its product family. (www.cisa.gov)

A **one-time password (OTP)** is not synonymous with phishing-resistant authentication. The National Institute of Standards and Technology (**NIST**) states that OTP authentication is not phishing-resistant and identifies WebAuthn-based verifier-name binding as a phishing-resistant approach. For an owner, the useful question is which strongest supported method can actually be enabled and recovered. This guidance does not establish a login mechanism for any provider whose documentation has not supplied one. (pages.nist.gov)

A **device screen lock** is another distinct control. NIST distinguishes a local activation secret from a centrally verified password because the activation secret is not sent to the verifier. Treat a locked handset as evidence about local device access, not as proof that an independent provider account cannot change a forwarding destination. Similarly, an outbound caller-ID spam label is outside this acceptance test: it is not evidence that an inbound routing edit is authorized or blocked. (pages.nist.gov)

SIM protection must be checked against the precise subscription. T-Mobile's SIM Protection page excludes T-Mobile for Business and describes an exception for eSIM transfers on Apple devices. Its separately documented Port Out Protection covers additional account categories and must be added to each line. The worksheet should therefore record the actual mobile account type and enabled feature, rather than using a generic carrier-lock checkbox. (www.t-mobile.com)

Port-out authorization deserves its own record. AT&T documents a transfer PIN shared across the account numbers being transferred and a business-account primary-user requirement to request it. Xfinity says its Number Lock blocks SIM swaps and port-outs for the mobile services it names, and separately describes email and text alerts for requests. Those claims support questions about the relevant mobile account; they do not establish universal hosted-number freezes or an alert for an inbound-menu edit. (www.att.com) (www.xfinity.com)

Use these acceptance prompts when comparing controls:

- **Action:** Name the exact change being restricted, not simply account security.
- **Scope:** Identify the product, account type, number, line or routing object covered.
- **Actor:** Record who can enable the protection and who can remove it.
- **State:** Verify whether it is enabled now, rather than merely available.
- **Exception:** Request the documented override and support-assisted workflow.
- **Evidence:** Keep the relevant provider response and demonstration result.

- **Alert independence:** Establish whether the change actor can also suppress monitoring.
- **Recovery:** Confirm who can restore control without the affected number.
- **Review:** Set a business-defined date to recheck enabled status.

Separate Audit Logs from Independent Change Alerts

An **audit log** supports retrospective inspection. An **alert** is intended to bring an event to someone's attention. A vendor may document one without establishing the other. Dialpad's Event Changelog is an administrator capability, with company or office exports and an emailed download link. The email delivering an export should not be counted as proof that each routing change proactively notifies an independent owner.

(help.dialpad.com)

Configuration evidence can be more useful than a generic activity timestamp. **8x8** documents Admin Console audit-event details showing previous and current modified values. Ask for a supported interface demonstrating the corresponding object in the proposed service: who changed it, what changed, when it changed and whether the old destination remains visible. Also ask whether a failed or denied administrative attempt is recorded; do not assume every event has the same coverage. (docs.8x8.com)

RingCentral's developer documentation says its Audit Trail API tracks the same configuration changes as the administrator interface, while labeling the API beta. Its separate Labs app lists company- or user-level forwarding changes among notification events. Crucially, the listing describes Labs apps as community projects, not officially tested or documented products, with no RingCentral support. These are examples of different evidence channels, not a recommendation to rely on that app for production account protection. (developers.ringcentral.com) (www.ringcentral.com)

Independent should be an observed property, not a product adjective. Ask whether the routing administrator can alter or remove the alert recipient, whether changing that recipient triggers another notification, and whether the recipient remains reachable if the business number or primary mailbox is unavailable. AT&T documents email to the primary account holder and texts to active wireless numbers when its Wireless Account Lock is toggled. Verify those recipients and dependencies instead of assuming that multiple delivery channels automatically create independence. (www.att.com)

Request written answers for the following:

- **Event coverage:** Routing, voicemail-recipient, administrator and recovery changes separately.
- **Notification target:** The exact mailbox, number or supported application receiving each event.
- **Delivery evidence:** The event timestamp, receipt timestamp and observed delivery result.
- **Edit authority:** Who can disable monitoring or change its recipients.
- **Retention:** How far back records are accessible and whether record ceilings apply.
- **Plan eligibility:** Whether the quoted subscription includes the demonstrated capability.

A support response saying that activity is logged is incomplete until the business can locate the relevant event. Dialpad's documentation refers customers to pricing or support to establish feature eligibility rather than naming eligible plans in the retrieved changelog article. Resolve that uncertainty in the quote or acceptance record. (help.dialpad.com)

Run a Reversible Owner-Approved Acceptance Test

The following is a recommended acceptance procedure, not a claim about a provider's supported test environment. Arrange a provider-supported demonstration on a test number or isolated temporary route. Obtain owner approval for the actor, supported interface, planned destination and undo method before making changes. If a safe isolated demonstration is unavailable, request a vendor demonstration and record the remaining uncertainty. Do not redirect live customer calls to prove a control exists.

Use the test to connect permission evidence to actual routing behavior. A named administrator should show the specific object and permitted action. Where a staff role is expected to lack change access, the provider can demonstrate that restriction through its supported interface. Teams' documented combination of object authorization and an assigned voice applications policy illustrates why showing only a role label is insufficient. Do not probe unauthorized endpoints or attempt to bypass restrictions. (learn.microsoft.com)

Keep the test record private and use these fields:

- **Owner approval:** Approver, permitted scope and planned test window.
- **Actor:** Named test administrator and displayed role or object authorization.
- **Interface:** Supported portal, application or provider-led demonstration.
- **Planned change:** Temporary destination or greeting on the isolated test object.
- **Observed route:** Result of an external call, including the expected recipient.
- **Audit evidence:** Event identifier, timestamp and redacted change details, if offered.
- **Alert evidence:** Recipient, arrival time and whether that recipient is independently reachable.
- **Undo result:** Restored configuration and successful repeat external call.
- **Decision:** Accepted, unresolved, or rejected against the owner's stated requirements.

For voicemail, test the documented delivery destination separately from the ringing destination. Confirm that a person receiving a voicemail notification has the intended information access. Google's ring group settings, for example, include additional recipients of after-hours email notifications. That is notification configuration; it should not be mistaken for proof of administrative authority or proof that the same address receives security-change alerts. (knowledge.workspace.google.com)

Where a provider offers before-and-after audit details, compare them with the planned change and undo result. The 8x8 Admin Console example demonstrates the kind of visible evidence to request, but does not establish identical fields in another service. A missing test alert remains unknown until the provider confirms whether the event is supported, how it is configured and how delivery can be demonstrated. No alert result in this worksheet should be converted into a guaranteed response time. (docs.8x8.com)

Exclude real number ports, SIM swaps, destructive account recovery and production security lockouts from the exercise. A support-assisted ownership change can have prerequisites that make a casual test inappropriate: Twilio's documented process, for example, requests affected account identifiers and the new owner's email when self-service transfer cannot be completed. Verify the recovery procedure through written evidence and a supported demonstration instead. (help.twilio.com)

Maintain Recovery, Offboarding and an Unexpected-Change Procedure

Build a **private recovery dependency map** before a problem occurs. For each public-number, mobile and email account, record the recognized owner, authorized backup, support channel, required recovery evidence and dependencies. Draw links showing which mailbox or number is needed to restore another account. Then ask whether losing any single dependency leaves an authorized person unable to reach the controls that restore it. This is a planning exercise, not a claim that a different recovery email alone solves every dependency. Google's distinct-address recommendation is a starting point. (support.google.com)

Keep secrets outside the shared worksheet. NIST describes saved recovery codes as intended for secure offline maintenance. Google explains that a used backup code becomes inactive and that generating a replacement set invalidates the old set. If the selected provider supports backup codes, use its documented storage and replacement procedure; record only the secure storage reference and responsible custodian in the operational map. (pages.nist.gov) (support.google.com)

Staff departure requires separate checks for administrative authority, notification access and remaining call destinations. Google's Workspace guidance illustrates the distinction: it recommends removing recovery email addresses and phone numbers, resetting sign-in cookies and revoking application authorization tokens. Those are Google-specific steps, not a universal phone-provider logout procedure. Ask each relevant provider which supported actions terminate existing access, and apply lawful employment and records procedures appropriate to the firm. (support.google.com)

Use a departure checklist that separates the following:

- **Administration:** Remove unnecessary roles, delegated access and invitations.
- **Sessions:** Revoke access through the provider's supported session and application controls.
- **Recovery:** Replace departing staff recovery channels and confirm the recognized backup.
- **Notifications:** Review shared mailbox membership and security-alert recipients.
- **Destinations:** Remove stale mobile routes and check overflow and voicemail destinations.
- **Continuity:** Place external calls through the remaining menu paths after approved changes.

Unexpected loss of calls is a symptom, not a diagnosis. First inspect the known greeting, route, business hours and voicemail settings, and check the provider's status information. Test from an outside phone and document the observed behavior. Contact support through a previously verified provider channel, preserve redacted timestamps and configuration evidence, and use the firm's outage procedure to communicate an approved alternative contact route. Do not assume a number transfer solely because calls stopped.

If an unexpected configuration change is confirmed, ask support to preserve the available event history and verify the authorized restoration process. Audit detail showing previous and current values can help distinguish what was changed from what was intended, as documented in 8x8's Admin Console. Keep account identifiers and ownership evidence available securely, without putting passwords, transfer PINs, one-time codes, recordings or former employees' personal information into a shared log. (docs.8x8.com)

Data Analysis and Evidence

The quantitative evidence here concerns **documented control limits**, not probabilities of loss or estimated savings. It cannot establish that one provider prevents more unauthorized changes than another. *Table 3* collects the numerical limits most useful for planning delegation, evidence retention and a legitimate transfer. Each value is tied to the named service and documentation scope.

Documented measure	Verified value	Decision implication and limitation
Teams authorized users	Maximum 15 per auto attendant or call queue. (learn.microsoft.com)	A delegation limit, not a limit on people who can answer calls.
RingCentral Audit Trail API history	Up to 180 days per account. (developers.ringcentral.com)	An API retention limit; it does not establish the same retention in the administrator interface.
RingCentral Audit Trail API volume	10,000 total records per account. (developers.ringcentral.com)	The ceiling may be reached before the time window ends.
8x8 audit review and query windows	Past 90 days , with queries limited to 30 days . (docs.8x8.com)	Retrieving the full documented period requires separate queries, not one assumed continuous export.
AT&T Number Transfer PIN validity	4 days , or 14 days for business accounts . (www.att.com)	Credential validity is not a promised porting-completion time or restoration deadline.
Nextiva NEXT role taxonomy	4 roles : User, Agent, Supervisor and Global Administrator. (help.nextiva.com)	Role count does not measure how narrowly each action can be delegated.

These figures measure different things and should not be combined into a security score. A longer history can assist review, but record ceilings and event coverage remain relevant. A larger role taxonomy does not prove that routing, voicemail, recovery and number transfer are separately permissioned. Nextiva's administrator interface includes user-level forwarding and call-routing settings; that tells the buyer where to request a demonstration, not whether a particular employee should receive the whole administrator role. (help.nextiva.com)

Licensing is another boundary to price explicitly. Microsoft's Queues app documentation names Teams Phone and Teams Premium requirements, while Zoom's role page requires a Phone license for users assigned Phone roles. Those conditions apply to the documented management workflows. They do not support multiplying an inbound-only firm's staff count by a suite seat price when staff merely answer calls on existing mobiles. Request a quote for the actual administrator, recipient and feature configuration. (learn.microsoft.com) (support.zoom.com)

No comparable current vendor price quotes or measured administrative-effort data were established for this acceptance exercise. A useful cost worksheet therefore leaves subscription charges, required administrative licenses, setup work and recurring review effort for the owner to enter from current quotes and observation. Do not populate it with invented breach probabilities, recovered revenue, fraud-prevention percentages or alert-response benchmarks.

The same restraint applies to controls that are merely available. Verizon explicitly states that its documented SIM Protection and Number Lock features are not enabled by default. An inventory entry should consequently distinguish **available**, **enabled and verified**, and **unknown**. These states are more informative than a binary comparison that gives every advertised feature full credit without checking the account. (www.verizon.com)

Implications and Future Directions

The purchasing decision is whether a provider's demonstrated administration and recovery model meets the firm's requirements. Establish those requirements before comparing subscription totals. A firm may accept a simpler arrangement if it can identify authorized administrators, maintain recovery access and tolerate the documented monitoring limitations. If independently delivered routing-change alerts or narrowly separated roles are mandatory and cannot be demonstrated, evaluate a fuller platform or another provider with suitable supported controls.

Granular delegation deserves careful evaluation rather than automatic adoption. Teams shows that permission can depend on both the authorized voice application and a policy. Quo separates workspace roles from phone-number access. These examples suggest asking for an action matrix tied to the actual number, instead of accepting a vendor-wide role description as sufficient evidence. More settings also create more items to review during onboarding and departure; the owner should account for that effort rather than assume a richer platform administers itself. (learn.microsoft.com) (learn.quo.com)

Independent recovery should remain part of future reviews as personnel and devices change. A different recovery email is useful only when the business understands who controls it and how it is recovered. Google's recommendation to use a different sign-in and recovery address supports that first separation; the remaining dependency analysis is the firm's responsibility. A narrowly authorized backup owner or administrator should be assigned only if the provider supports that arrangement and the business can maintain it. (support.google.com)

Finally, distinguish **documented roadmap or experimental functionality** from accepted production controls. The RingCentral Labs listing expressly limits its official status and support. A business requiring monitored configuration changes should request the vendor's supported service, eligible plan, notification configuration and recovery process in writing. A future feature promise can remain a procurement question; it should not be recorded as an enabled safeguard or used to close an unresolved acceptance item. (www.ringcentral.com)

Frequently Asked Questions (FAQs)

Who can change business call routing?

Whoever has the relevant provider permission for the target number or routing object. It may be a delegated operator rather than a broad administrator. Google Voice documents a ring group management role; the business should request the equivalent scope for its own service and verify the actual assignment. (knowledge.workspace.google.com)

Do people answering calls need administrator accounts?

Receiving calls and administering the public number are different responsibilities in this worksheet. Do not issue management access simply because someone answers a routed call. Where end-user accounts exist, review their narrower settings too: Ooma documents voicemail, logs and preferences for a user's own extension, without establishing company-wide administration through that page. (www.ooma.com)

What proves that call routing permissions are restricted?

A provider-supported demonstration showing the proposed role can perform the allowed action and cannot perform a prohibited one, within the authorized test scope. Keep the object assignment and policy evidence. Use the demonstrated assignment and configuration scope as the acceptance evidence.

What is business phone number porting authorization?

For this operational checklist, it is the provider's documented authority and credential process for a legitimate transfer. It is separate from permission to edit a menu. AT&T's business guidance reserves requesting its Number Transfer PIN to the primary user. Confirm the actual provider's process and do not treat possession of a code as a determination of legal business rights. (www.att.com)

How should a business secure a phone account?

Map administrators, destinations and recovery dependencies; use the strongest available supported authentication; verify enabled controls; test supported logs and alerts; and review access when staff change. CISA recommends stronger methods ahead of text or email codes when available. A phone provider's actual login and recovery options still require confirmation. (www.cisa.gov)

Conclusion

Business phone system access control should be accepted at the level of **observable actions**. The owner needs to know who can alter the public route, who can change voicemail access, who can modify recovery information, and who can authorize a transfer. Receiving customer calls should remain a separate responsibility from administering those settings unless a documented business need justifies combining them.

The three-layer map keeps the decision concrete. Review the public-number provider, the destination mobiles and the independent email or authentication channels used to recover them. A password, device lock, SIM feature, port-out control, log and alert each address different questions. None should receive credit for an action outside its documented scope.

Before purchase or renewal, obtain written answers, identify unknowns and approve a reversible demonstration. Record the actor, intended change, observed route, available audit event, alert recipient and successful undo. Maintain a private recovery map and repeat the relevant access and destination checks when staff leave or responsibilities change.

The final acceptance question is straightforward: **If someone changes where customer calls go, how will the owner know, and can an authorized person regain control?** Accept the service only when the documented answers fit the firm's requirements. Where a required control remains unknown, resolve it with the

provider or select an option that can demonstrate it.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. <https://learn.microsoft.com/en-us/microsoftteams/aa-cq-setup-authorized-users>
2. <https://learn.quo.com/setting-up-quo/adding-and-onboarding-your-team/add-users-assign-roles>
3. <https://www.verizon.com/business/support/account-maintenance-and-management/my-business-wireless-account-management/mobile-security-management>
4. <https://www.t-mobile.com/support/plans-features/sim-protection>
5. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>
6. <https://help.dialpad.com/hc/en-us/articles/54742369347611-Event-Changelog>
7. <https://developers.ringcentral.com/guide/account/audit-trail>
8. <https://www.ringcentral.com/apps/audit-trail-notifications>
9. <https://support.google.com/accounts/answer/183723?hl=en>
10. https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0070100
11. https://knowledge.workspace.google.com/admin/voice/make-a-voice-user-a-ring-group-manager?hl=en&rd=1&visit_id=639177347881111277-1298913941
12. <https://help.nextiva.com/article/next-2-0-administrator-settings>
13. <https://learn.microsoft.com/en-us/microsoftteams/aa-cq-manage-voice-applications-policies>
14. <https://www.att.com/support/article/wireless/000102016>
15. <https://www.t-mobile.com/support/account/transfer-your-phone-number>
16. <https://support.google.com/accounts/answer/1187538?hl=en>
17. https://knowledge.workspace.google.com/admin/voice/edit-ring-groups?hl=en&rd=1&visit_id=639177347886044075-1816080121
18. <https://www.ooma.com/small-business-phone-systems/features-support/end-user-portal-overview>
19. <https://help.twilio.com/articles/223183428-Can-I-change-the-owner-of-the-account->
20. <https://pages.nist.gov/800-63-4/sp800-63b.html>
21. <https://www.att.com/support/article/wireless/KM1447526>
22. <https://www.xfinity.com/hub/mobile/sim-swap-port-fraud>
23. <https://docs.8x8.com/8x8WebHelp/admin-console/Content/audit-events.htm>
24. <https://support.google.com/a/answer/6329207?hl=en>

THE PUBLISHER

About Auto Attendant

Auto Attendant gives a small business one phone number and a recorded menu that sends each caller to the right person. The call rings the mobile that person already carries, using their normal dialler and their normal mobile plan. Pricing is a single flat monthly fee for the whole company rather than a charge for each user, and there is no app, desk phone or hardware to install.

One number, one menu, the phones you already own

A caller dials the business number, hears a short greeting and chooses an option. Each option can ring one mobile, ring several at once so whoever is free answers first, or try people one after another in a set order. There is no limit on how many people sit on the receiving end, because nobody is billed per seat. Setup is done by the owner in a few minutes: pick a number, write the greeting, and point each option at a mobile.

What it deliberately is not

An auto attendant routes a call; it does not answer one. Nobody at Auto Attendant speaks to callers, and no AI stands in for a receptionist. A business that wants its calls handled, messages taken and appointments booked wants an answering service, which is a different product at a different price. A business that needs call recording, queues, agent dashboards or CRM integration wants a contact centre platform. Auto Attendant is for the case where the call should simply reach the right pocket.

Keeping personal numbers off the internet

The business number is the only number a caller ever sees. Personal mobile numbers are never displayed and never given out, which is what lets an owner put a number on a website, an invoice, a van or a Google Business Profile without handing a personal line to everyone who finds it. An existing advertised number can be ported across and kept, and the old line keeps working while the port is in progress.

Work with Auto Attendant

Visit [Auto Attendant](#) to see [how it works](#), [how it compares](#) to a personal mobile, Google Voice and a full phone platform, and the current [pricing](#).

Telephone number portability, emergency calling and caller-ID rules differ by country and change over time. Articles published here describe general practice and cite primary regulator and carrier sources; they are not a guarantee of any timeline, and they are not legal or regulatory advice for a specific business.

Website: <https://autoattendant.io>

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.