RingCentral

What's In Deck 24.4 AT&T Office@Hand

24.4 Table of Contents

Desktop/Web Apps

- Mute SMS conversation
- Favorite SMS conversation
- Change name of group MMS conversation
- New voicemail setting entry point
- New entry point to create new contact in Desktop app
- Download faxes from bulk editing view
- Audio and Video Messaging
- Closed captions and live transcription during phone calls

Admin & Core

- Bulk delete unassigned extensions
- Assign CNAM to specific phone numbers
- Assist Customer with Company CNAM Registration
- Ability to set caller ID for all phones / features
- Role-based MFA (using authenticator app) policy
- Update Service Web UI for Change Password, PIN, and Security Question
- Restrict GeoIP/IP for App & ServiceWeb
- User-level toggle to restrict site numbers as caller ID
- Delete User Flow: Reassign and Delete Numbers
- Purchase Type field rename for Device Information

Integrations

- SFDC Leave Conference as Host

Call Handling

- Site Call Recording Settings
- Site and Call Queue call handling templates
- Disable ability for Agents to turn off Accept Queue Calls toggle
- Enable delegated lines feature for partner brands

Analytics

- Business Analytics - Sharing a dashboard "As Is"

Hardware

- Firmware update

24.4 Deployment Schedule - AT&T Office@Hand

Item	Release	Dates	Status	Comments
Admin, New Licenses, New Hardphones	24.4	11/22		
Office@Hand Mobile App	24.4.20	tbd		Handoff tbd
Office@Hand Desktop/Web App	24.4	12/3		

Desktop/Web Apps

Feature: Mute SMS conversation

What's new	• Ability to mute SMS conversation threads similar to muting functionality offered in Messaging today
What problem does it solve	• Distraction of SMS conversation threads that user doesn't want to be bothered by
Rollout plan	• 24.4.20

Feature: Mute SMS conversation
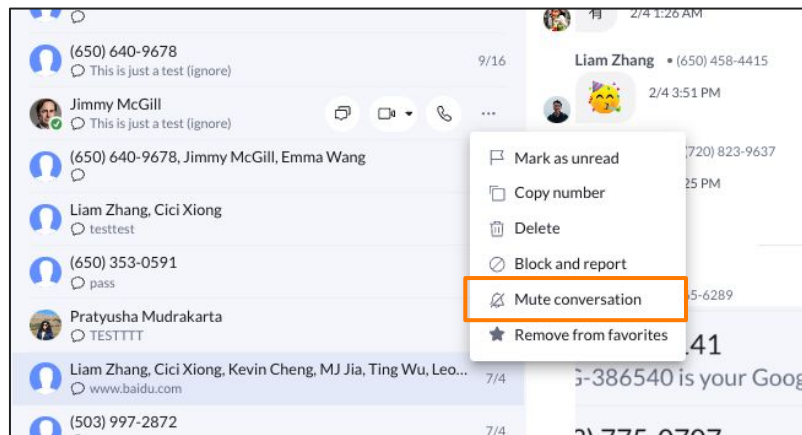
Mute / Unmute conversation.
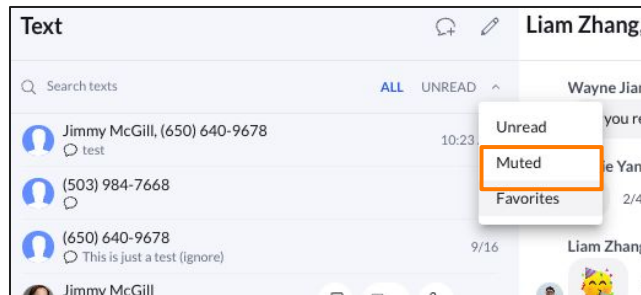
Show only muted conversation using existing filter pattern
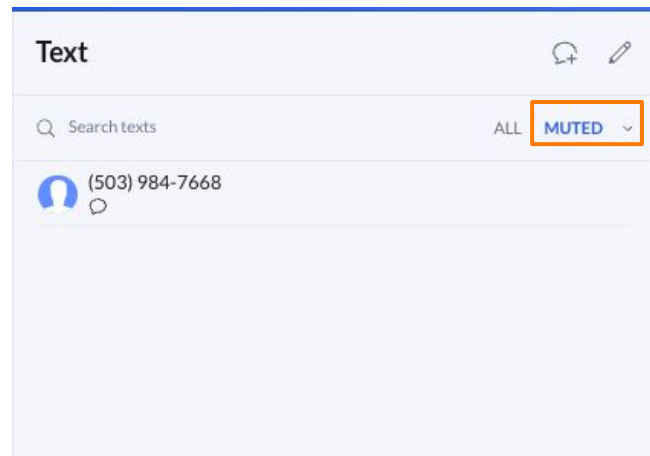
Feature: Favorite SMS conversation

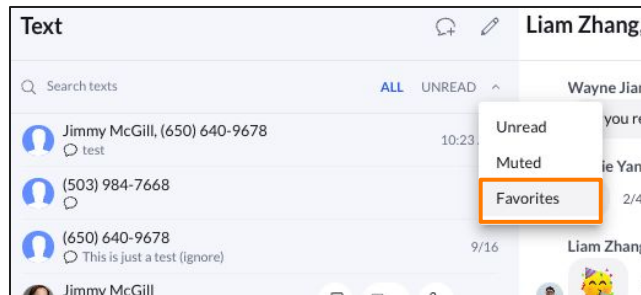|	
What's new	• Ability to favorite SMS conversation threads similar to favoriting functionality offered in Messaging
What problem does it solve	• Difficulty finding highest priority SMS conversation threads
Rollout plan	• 24.4.20

Feature: Favorite SMS conversation
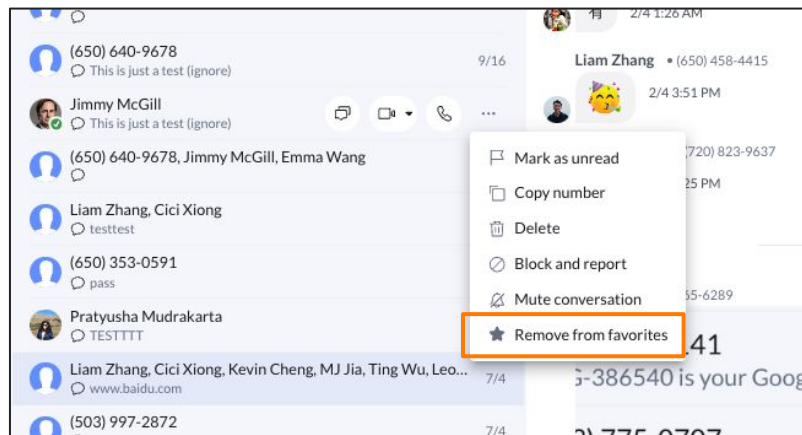
Add / remove to favorites from list of quick actions.

Show only favorites conversations using existing filter pattern
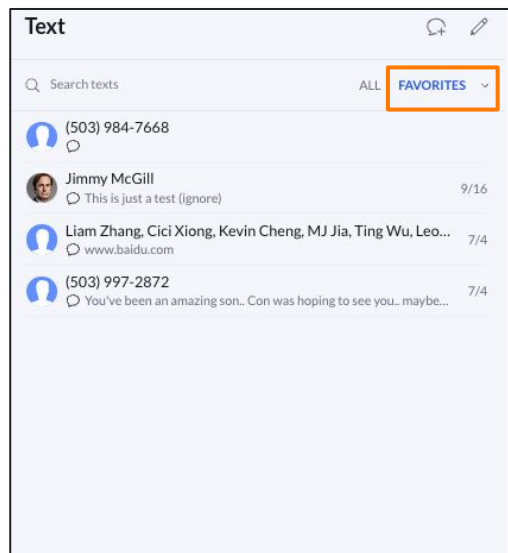
Feature: Change name of group MMS conversation

What's new	● Ability to rename a group MMS conversation

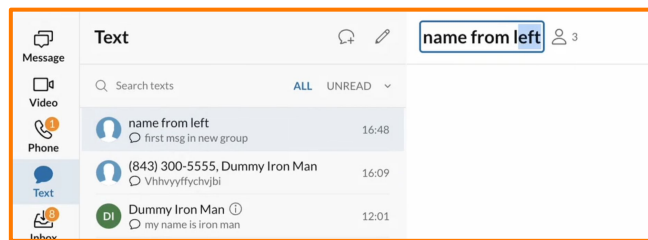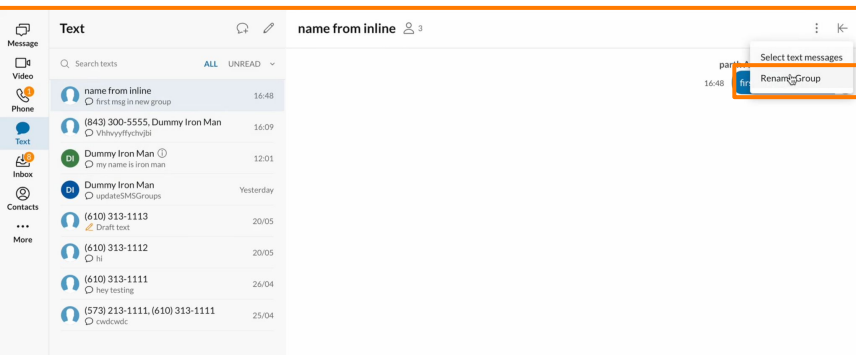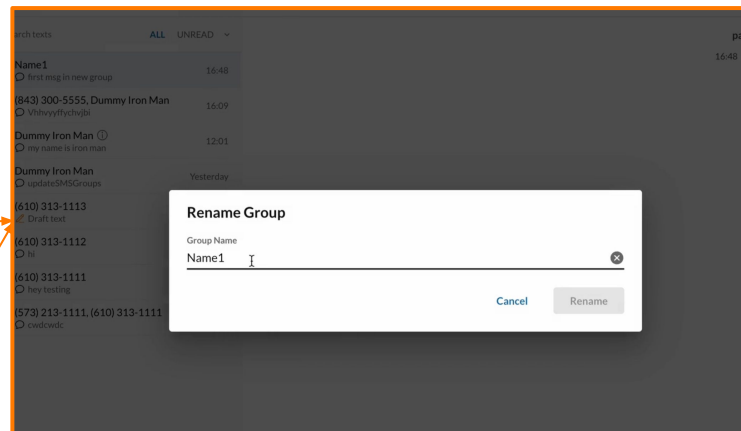| **What problem does it solve**	● Hard to identify SMS groups, closing a gap users have become accustomed to from native phone messaging apps (iOS, Android)

Rollout plan	● 24.4.20

Feature: Change name of group SMS conversation
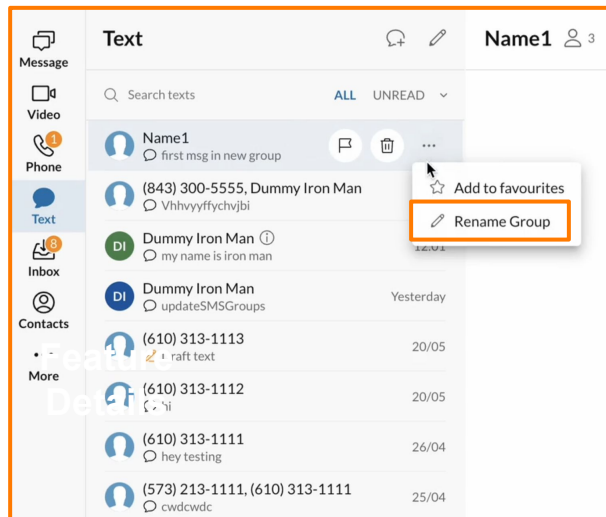
Two entry points that take you to the rename group window

As well as a third option to edit group name directly in header

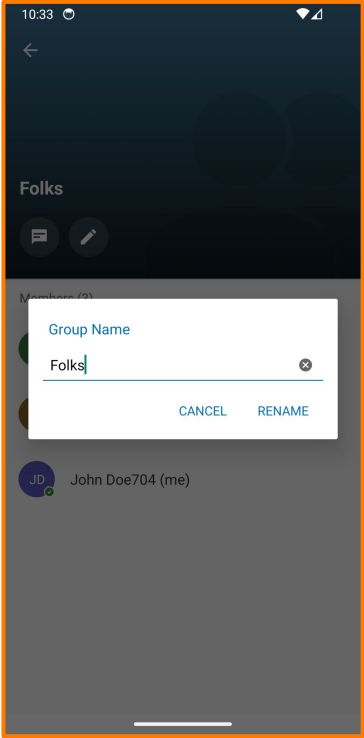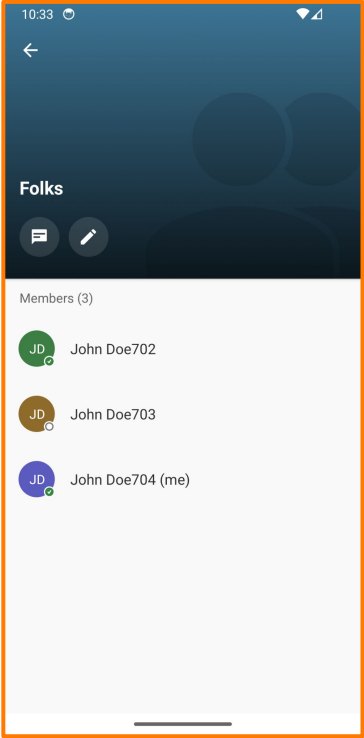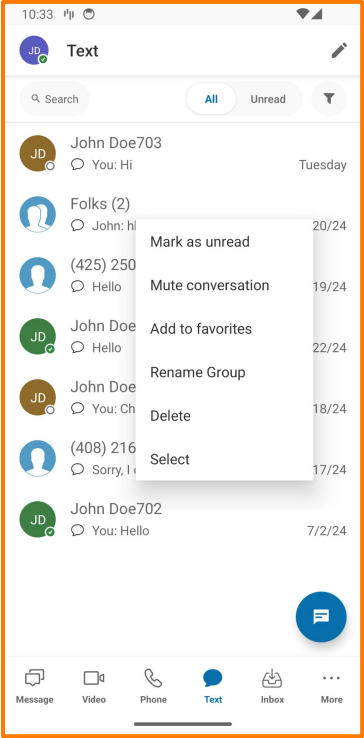Feature: Change name of group SMS conversation

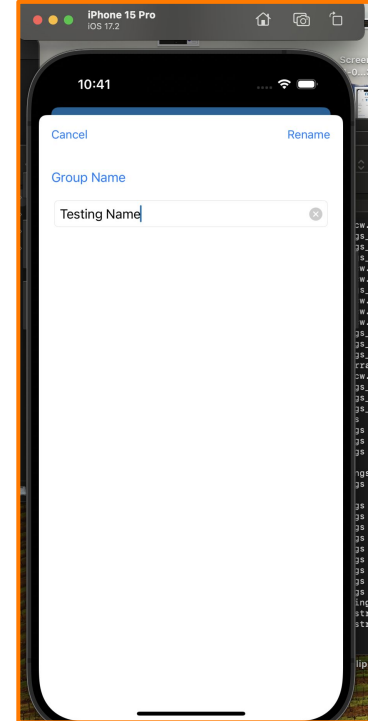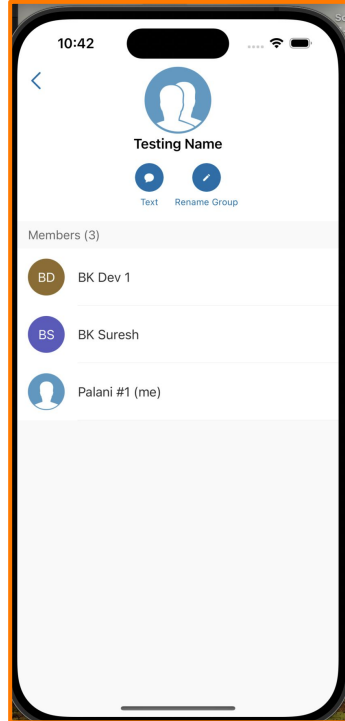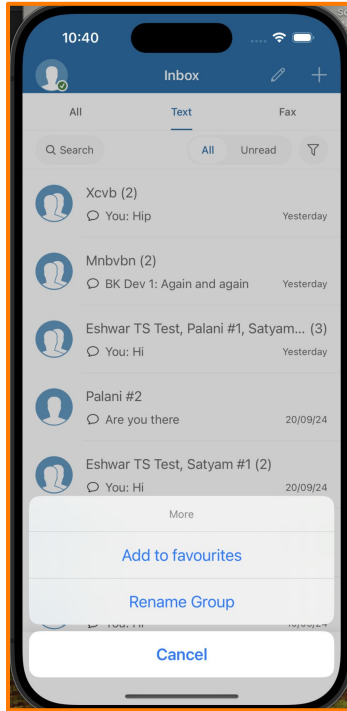Opportunity to add group name inside create group sms flow

Hidden when not sending group text

Feature: Change name of group SMS conversation

Android

Feature: Change name of group SMS conversation

iOS

Feature: New voicemail setting entry point

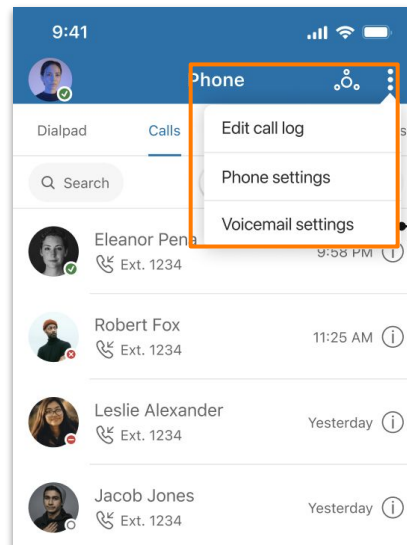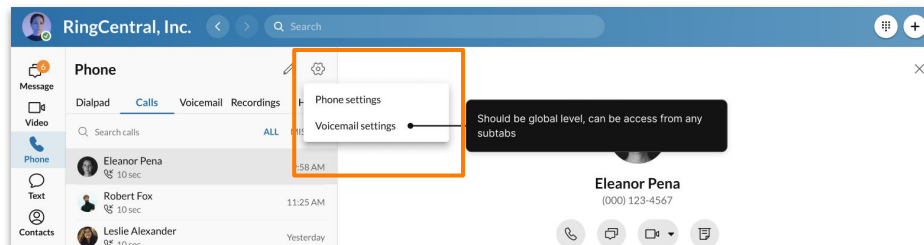| **What's new**	• Add "Voicemail settings" entry point directly in the UI where user access Voicemail (avoid digging around for this setting)

What problem does it solve	• Friction created when user tries to get to voicemail settings

Rollout plan	• 24.4.20

Feature: New voicemail setting entry point

Feature: New entry to create a new contact in Desktop app

What's new	• Quick entry point to create new contact / add number to existing contact when number in dialpad doesn't match any current contacts

What problem does it solve	• Improved usability to quickly add new contact while entering number into dialpad • Closes feature gap with Mobile app

Rollout plan	• 24.4.20

How it works

Feature: Download faxes from bulk editing view

What's new	• Ability to bulk download faxes while in the bulk editing view
What problem does it solve	• Cumbersome process of downloading faxes one by one
Rollout plan	• 24.4

Download faxes from bulk editing view

How it works
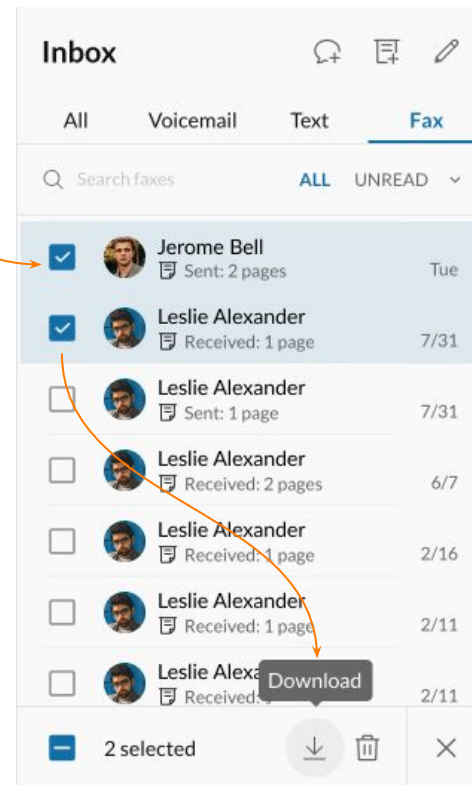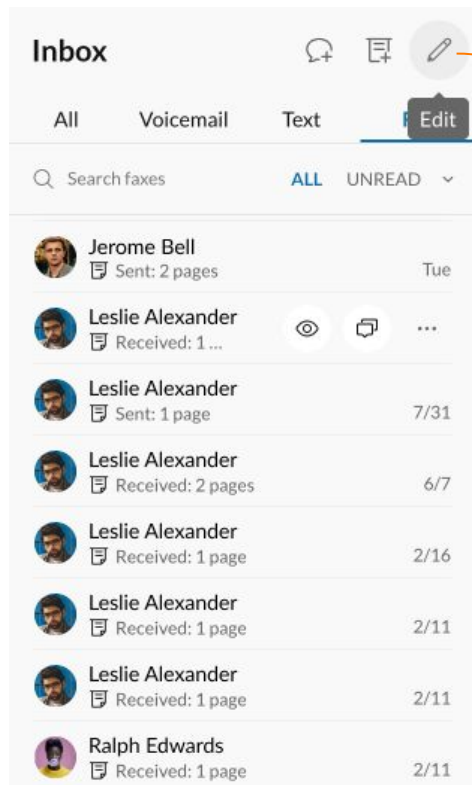
Feature: Audio and Video Messaging (GA)

What's new	• Now you can send audio and video messages to your contacts. Easily record and send an audio or video message to save time and add context to your conversations.

What problem does it solve	• Existing messaging feature offers no way to send a video or audio messages like most competitors, it is not hard to do using existing OS level features like audio recording, video record using cam/mic. • Supported by key competitors: Slack, MS Teams, Zoom Chat

Rollout plan	• **24.4.20**

Audio messaging - Desktop

How it works - Record audio message

©2021 RingCentral

Audio messaging - Desktop
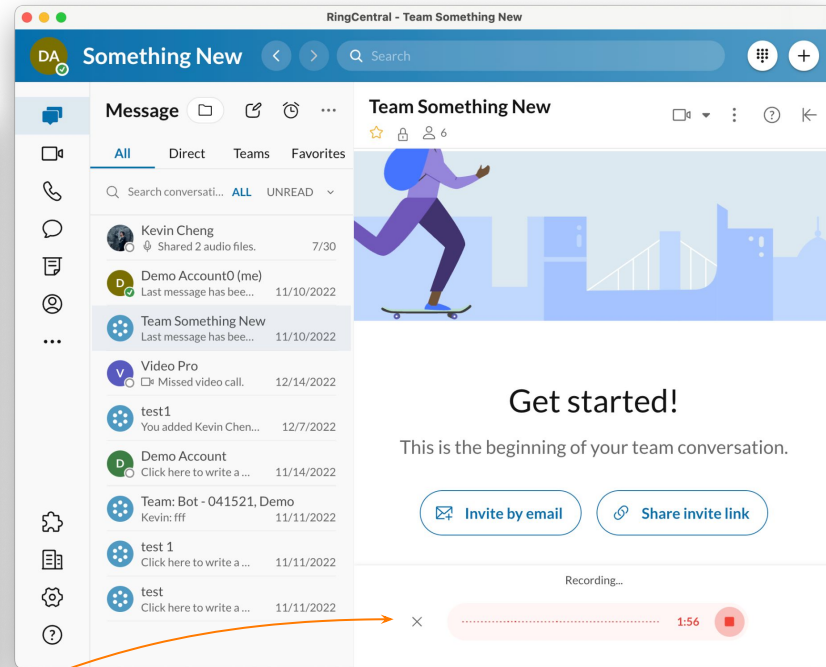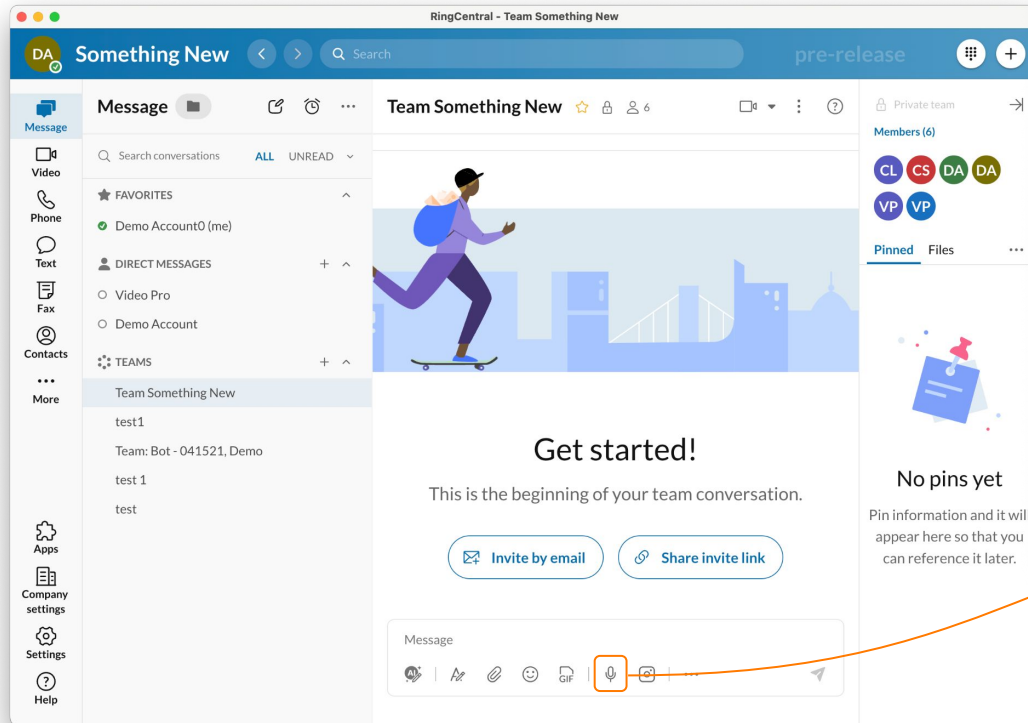
How it works - Send audio message

©2021 RingCentral
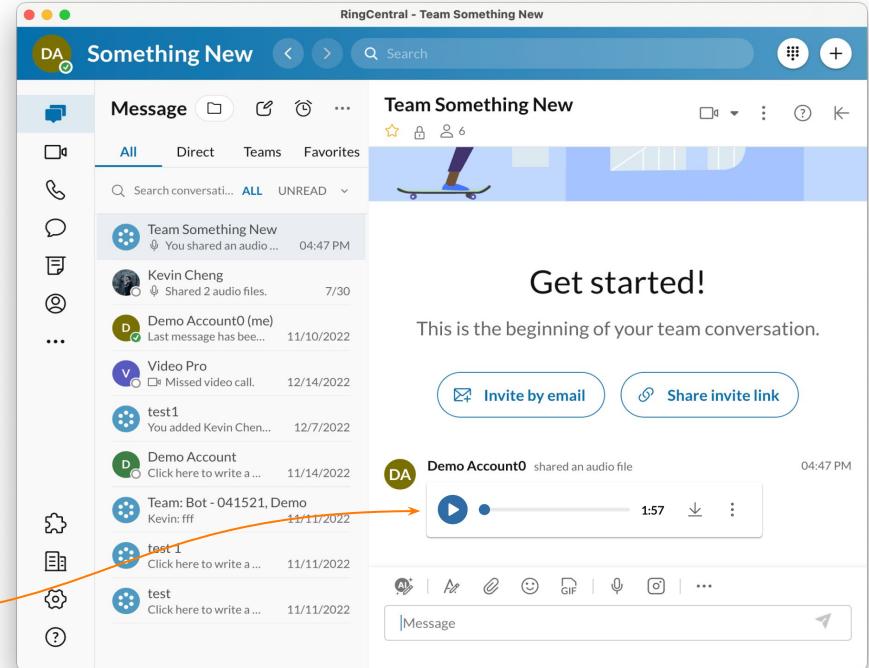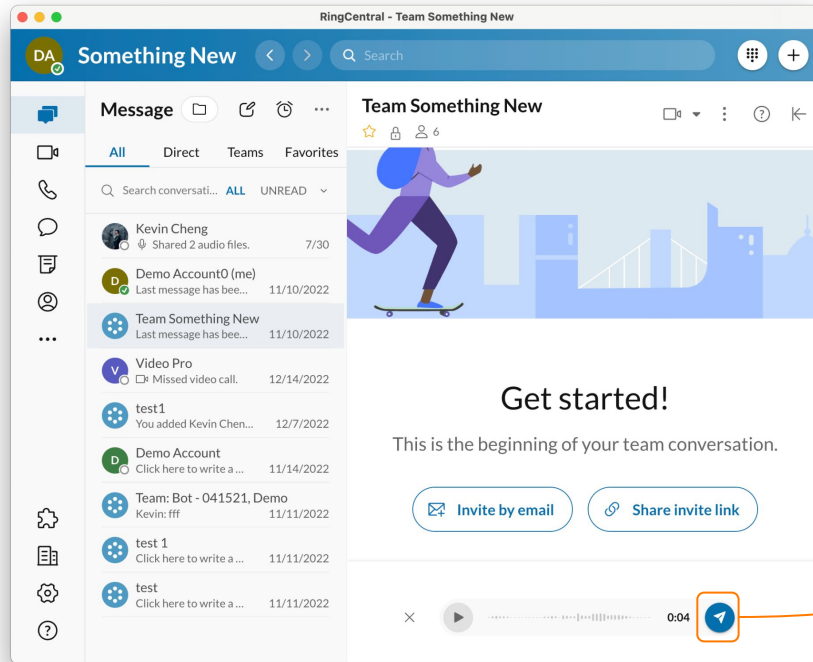
Video messaging - Desktop

How it works -
Record video message and share screen

©2021 RingCentral

Video messaging - Desktop
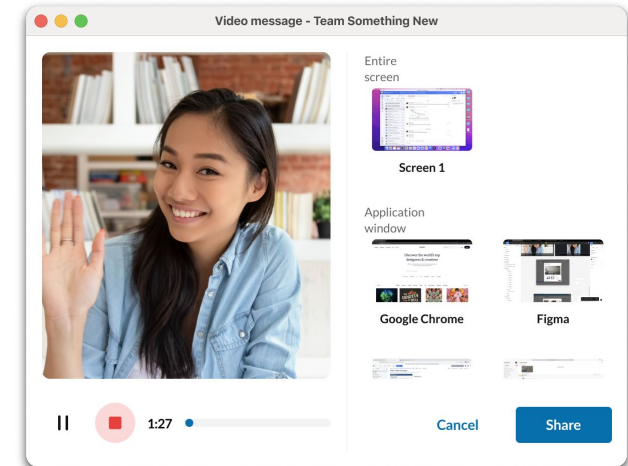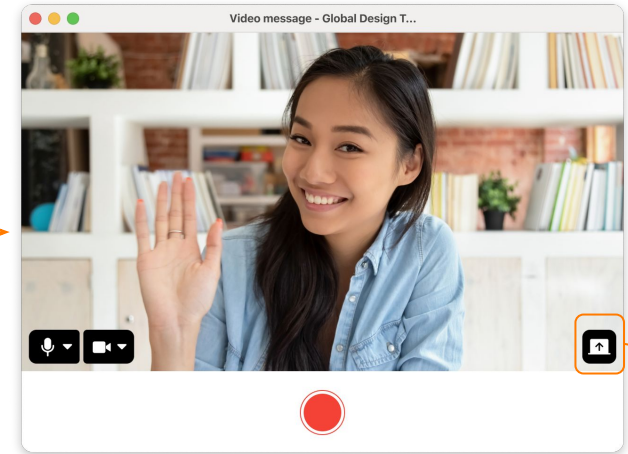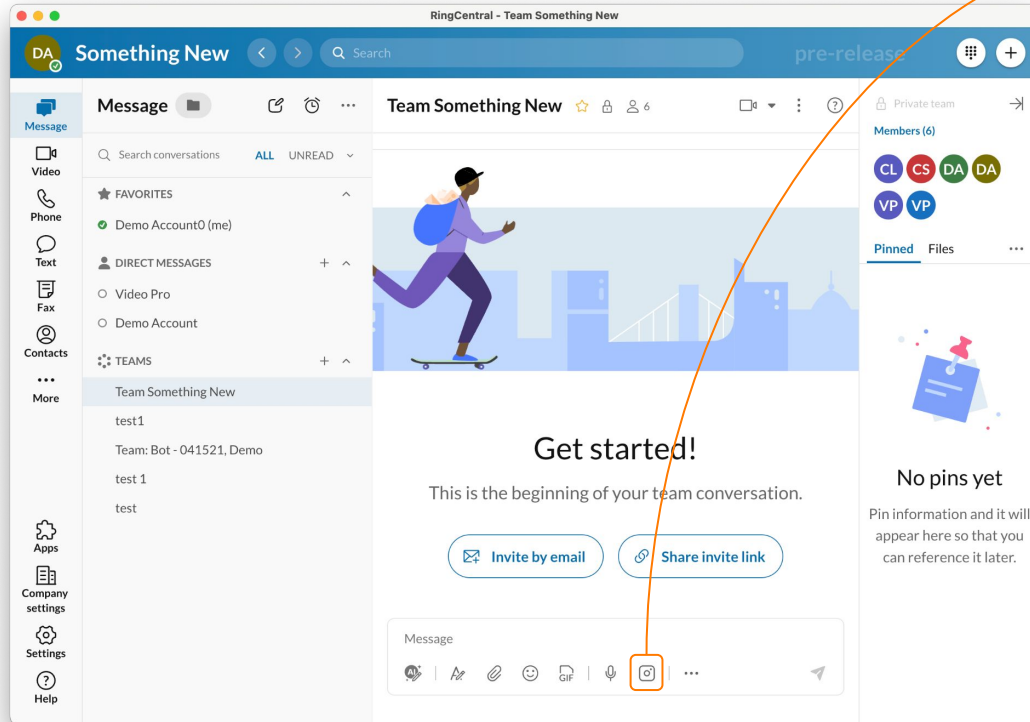
How it works - Send video message

©2021 RingCentral

How it works

Screen 1 (5:22):
Team Something New ▸

Welcome!

Work the way that you want from anywhere. The RingCentral app has everything you need to stay connected: team messaging, video meetings, and phone — all in one place.

Learn more

Share photos or videos

Message

Screen 2 (5:22):
Team Something New ▸

Welcome!

Work the way that you want from anywhere. The RingCentral app has everything you need to stay connected: team messaging, video meetings, and phone — all in one place.

Learn more

Share photos or videos

1:58

Screen 3 (5:22):
Team Something New ▸

Welcome!

Work the way that you want from anywhere. The RingCentral app has everything you need to stay connected: team messaging, video meetings, and phone — all in one place.

Learn more

Share photos or videos

0:03

Screen 4 (9:41):
Team Name ▸

Do we have a meeting to discuss Q2 planning?

Team, I scheduled a meeting to go through the Q2 planning tomorrow.

Mandy Lau — 3:20 AM
Julie Moon Sorry, I cannot attend today's weekly meeting. From the 09/08 note, I have comment for QA part. Any questions ping me cc: Bruce Lau

Andy Lee — 4:30 AM
Working at home today.

Bruce Lau — 11:10 AM
Could you let me know?

Jane Smith — 11:30 AM
0:30

Message

Video messaging - Mobile

How it works

Known Limitations

- **On Web app, Safari and Firefox are not supported regarding this feature.**

Feature: Closed captions and live transcription during phone calls

What's new	During a phone call in the Unified app, you can turn on closed captions and live transcription.
What problem does it solve	Closed captions and live transcripts can improve accessibility for your call, and help you catch up with anything you may have missed.
Rollout plan	• November 2024 (Desktop and Mobile) • Premium/Enterprise packages only • O@H 2.0 only

Feature: Closed captions and live transcription during phone calls

How to use closed captions during a phone call

During a phone call in the Unified app, you can turn on closed captions by clicking the **Turn on closed captions** icon (a) at the top right of the call window.

A panel will appear to the right, showing scrolling captions of what's being said on the call. Click the **Font size** icon (b) to make the text small, medium, or large.

To turn off closed captions, click the **Close** icon (c) at the top right of the caption panel, or click the **closed captions** icon (a) again.
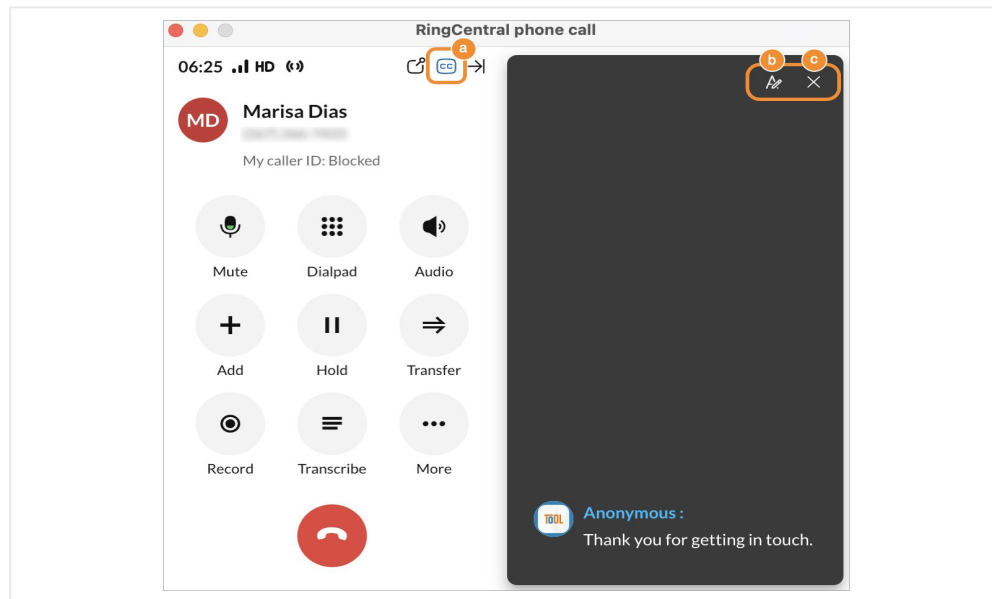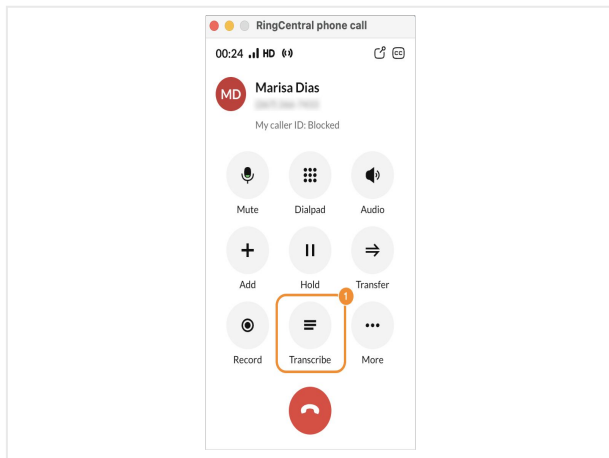
Feature: Closed captions and live transcription during phone calls

How to use live transcription during a phone call

1. During a phone call in the RingCentral desktop and web app, you can turn on live transcription.

   Click **Transcribe** on the dialpad.

2. The Call transcript will appear to the right, and a prerecorded voice will notify all parties on the call that transcription is on.

   a. Click the arrow at the top of the dialpad to show or hide the transcript window.
   b. Click the **Font size** icon to adjust the size of the transcript text.
   c. Click the **Download** icon to download a copy of the transcript so far.

3. To stop transcribing the call, click the **Stop Transc** button on the dialpad.
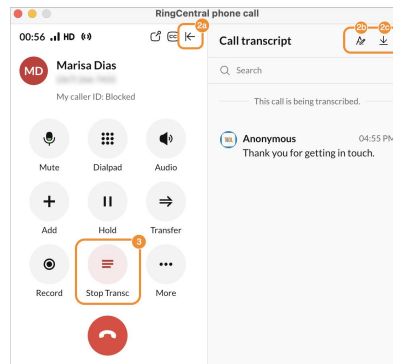
Admin & Core

Feature: Bulk delete unassigned extensions

What's new

Bulk delete unassigned extensions in SW

What problem does it solve

- Currently we only have single delete action for unassigned extensions. If the admin wants to delete obsolete unassigned extensions, he needs to go through the extensions one by one. The manual process is exceedingly cumbersome for bulk deletes.

Rollout plan

- GA in 24.4
- O@H 2.0
- All brands

Feature: *Bulk delete unassigned extensions*
How it works

- Customers could select multiple unassigned extensions in UI and delete them via bulk delete operation.

- The max number for bulk delete operation is 25.

User List » **Unassigned Extensions**

Search 🔍

+ Add Unassigned Ext ⋮

🗑 Delete

☑	Name	∨	Serial No.	Number	Actions
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1252	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1377	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1093	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1828	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1308	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1514	⋮
☑	Ext. with Avaya IX Conference Phone B199			(205) 624-1802	⋮

Feature: *Assign CNAM to specific phone numbers*

What's new

- Today, CNAM can only be assigned to all numbers on a per-Site basis.
- The goal of this feature is to allow customers to set CNAM on a per-number basis.

What problem does it solve

- Contact center customers often have different business identities, so they need the ability to set CNAM on a per number basis. As an Admin, I need the ability to assign CNAM per number, so I can override company/site CNAM.
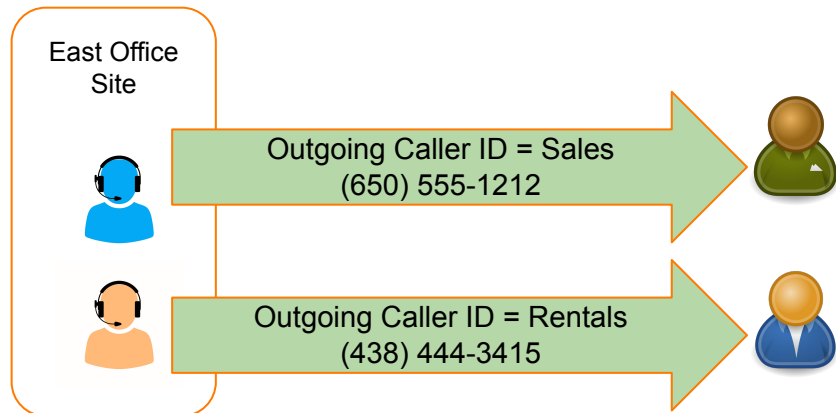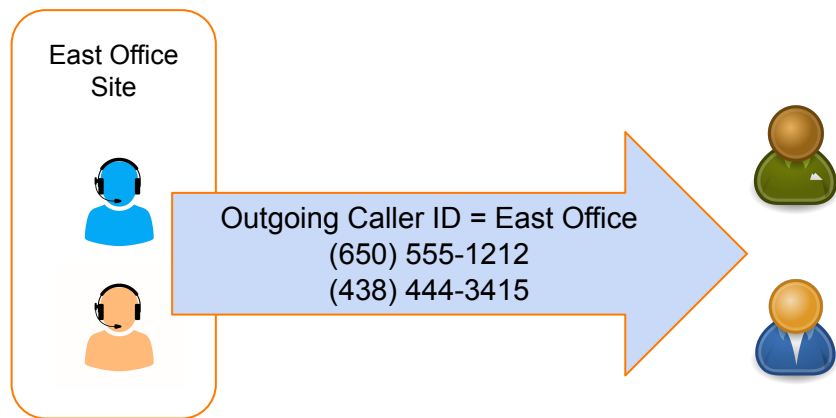
Rollout plan

- GA for all brands that support North American numbers
- Applies to all packages with calling capabilities
- No pricing impacts

How It Works

Today outgoing caller ID is configured for the company/site

Now outgoing caller ID can be configured for individual phone numbers

NEW SETTING TO USE SITE CNAM

In the **MAIN SITE** Caller ID Name
section has two new settings are
available
- Use the Main site caller ID
  name for Main site phone
  numbers
- Use the Main site caller ID
  name for all sites and phone
  numbers

These options allow the admin to
enforce new CNAM enforcement
options

NEW SETTING TO USE SITE CNAM

When
- Use the Main site caller ID name for Main site phone numbers

AND
- Use the Main site caller ID name for all sites and phone numbers

Are checked

On the Other Sites the selection will checked and locked

Phone Numbers for all sites will have the selection checked and locked

Set an outgoing caller ID name for phone numbers assigned to the Main site

◉ Use a custom caller ID name

> TYCO MOTORS

Main Site

○ Use a blank caller ID name. Outgoing calls may be marked as SPAM

☑ Use the **Main site** caller ID name for **Main site** phone numbers

☑ Use the **Main site** caller ID name for all sites and phone numbers

Set an outgoing caller ID name for phone numbers assigned to the Boston Office ⓘ

◉ Use the Main site caller ID name

> TYCO MOTORS

Other Sites

○ Use a custom caller ID name

☑ Use the **Boston Office** caller ID name for all **Boston Office** phone numbers

Caller ID Name ⓘ

◉ Use **Boston Office** caller ID name

> TYCO MOTORS

Phone Numbers

○ Use a custom caller ID name

NEW SETTING TO USE SITE CNAM

When

- Use the Main site caller ID name for Main site phone numbers

Is checked

Set an outgoing caller ID name for phone numbers assigned to the Main site

⦿ Use a custom caller ID name

TYCO MOTORS

◯ Use a blank caller ID name. Outgoing calls may be marked as SPAM

☑ Use the **Main site** caller ID name for **Main site** phone numbers

☐ Use the **Main site** caller ID name for all sites and phone numbers

Main Site

Phone Numbers for the main site will have the selection checked and locked

Caller ID Name ⓘ

⦿ Use **Main site** caller ID name

TYCO MOTORS

◯ Use a custom caller ID name

Phone Numbers
Of Main Site

NEW SETTING TO USE SITE CNAM

In the Caller ID Name section a new setting is available for Other Sites

- Use the "Site Name" of the other site caller ID name for all site phone numbers

NEW SETTING TO USE SITE CNAM

In the Phone Number section a new setting is available for Calling ID Name allowing for a Custome CLID to be set per Number

Feature: *Assist Customer with Company CNAM Registration*

What's new

- Today, some customers report their outgoing calls do not reflect their desired CNAM and may be displayed as SPAM.
- The goal of this INIT is to provide the customer with better guidance and tools to help them register with the Free Caller Registry. https://freecallerregistry.com/fcr/

What problem does it solve

- Free Caller Registry enables entities making legitimate outbound phone calls to submit their data to the three major providers of call management services supporting the major US wireless carriers once via a standard, centralized experience.

Rollout plan

- 24.4.2 minor
- GA for all brands that support North American numbers
- Applies to all packages with calling capabilities
- No pricing impacts

NEW OPTION TO EXPORT COMPANY CNAMs

In the **MAIN SITE** Caller ID Name section a new Register your phone numbers with "Free Caller Registry" is available

By clicking on Free Caller Registry, this will open a new window that would allow to download the number to CNAM mapping in the format expected by Free Caller Registry as well as provide the link to Free Caller Registry

NEW OPTION TO EXPORT COMPANY CNAMs

In Desktop app in **Company Info** under Caller ID Name section a new Register your phone numbers with "Free Caller Registry" is available

By clicking on Free Caller Registry, this will open a new window that would allow to download the number to CNAM mapping in the format expected by Free Caller Registry as well as provide the link to Free Caller Registry
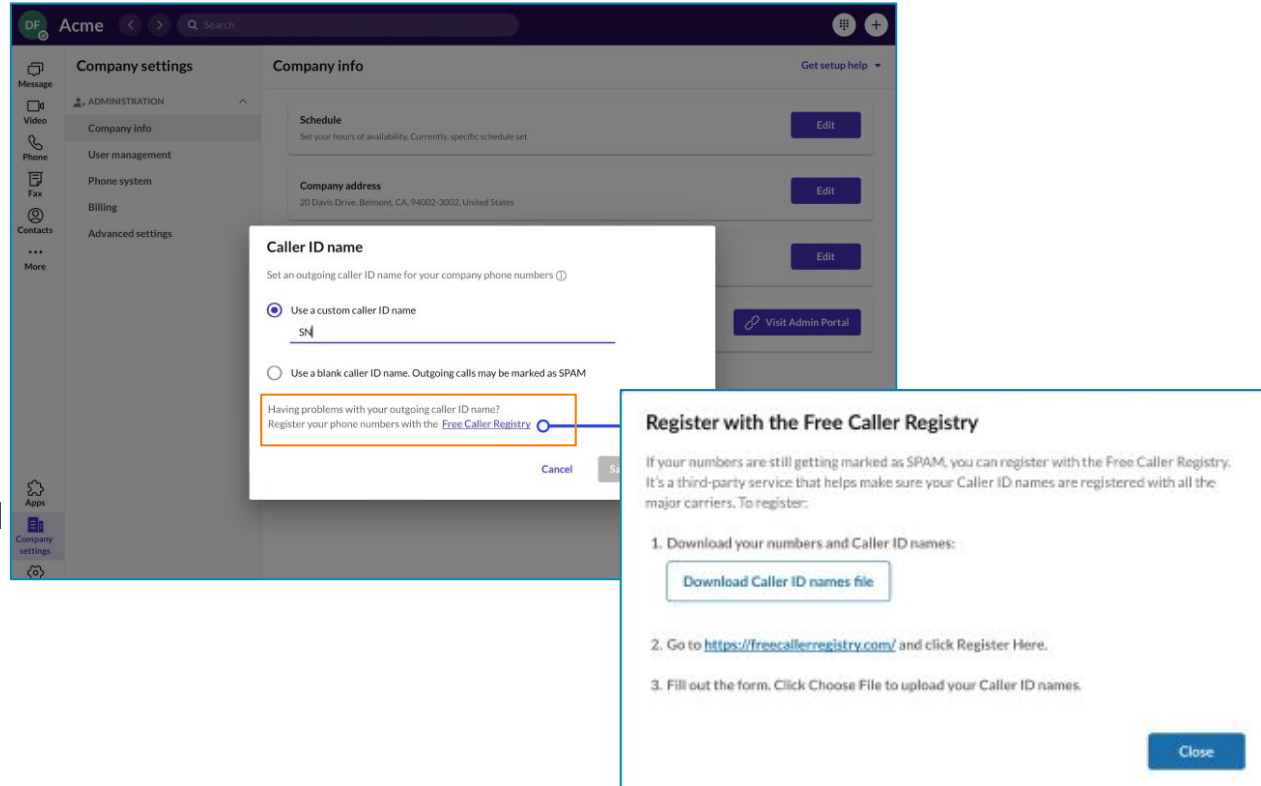
Feature: *Ability to set caller ID for all phones / features*

What's new

- Customer admins (Service Web admins) and end customers (Service web MyExtension users) now have the ability to set caller ID for all phones or features at once.
- INIT-12962

What problem does it solve

- Previously a user had to update the caller ID settings one by one, or use bulk caller ID capabilities (which is sometimes overkill for some quick ad-hoc changes and also not available to end customer)

Rollout plan

- 24.4
- All Brands
- All Packages supporting caller ID

Ability to set caller ID for all phones / features

View Number activation status (bulk)

- Only phone numbers compatible with all phones or features will be displayed
- Same caller ID restrictions apply per existing feature

©2024 RingCentral

Feature: Role-based MFA (using authenticator app) policy

What's new
- Administrators can enforce multi-factor authentication (MFA) for specific roles. This security measure requires users to complete a second authentication step using a time-based one-time password (TOTP) generated by authenticator apps such as Google Authenticator.

What problem does it solve
- Offers flexibility in enforcing this rule, such as applying it only to privileged roles rather than to all users.

Rollout plan
- GA: 24.4.2 minor
- All brands

Enforce MFA policy on selected roles

- When enabling the MFA policy in the Admin Portal, administrators will be presented with two options:
  - All user roles
  - Selected user roles only

- The list of roles is identical to those found under Users->Roles

- Two-factor authentication will appear in the left navigation even if an SSO policy is enforced, accompanied by a note indicating it cannot be used due to SSO policy enforcement
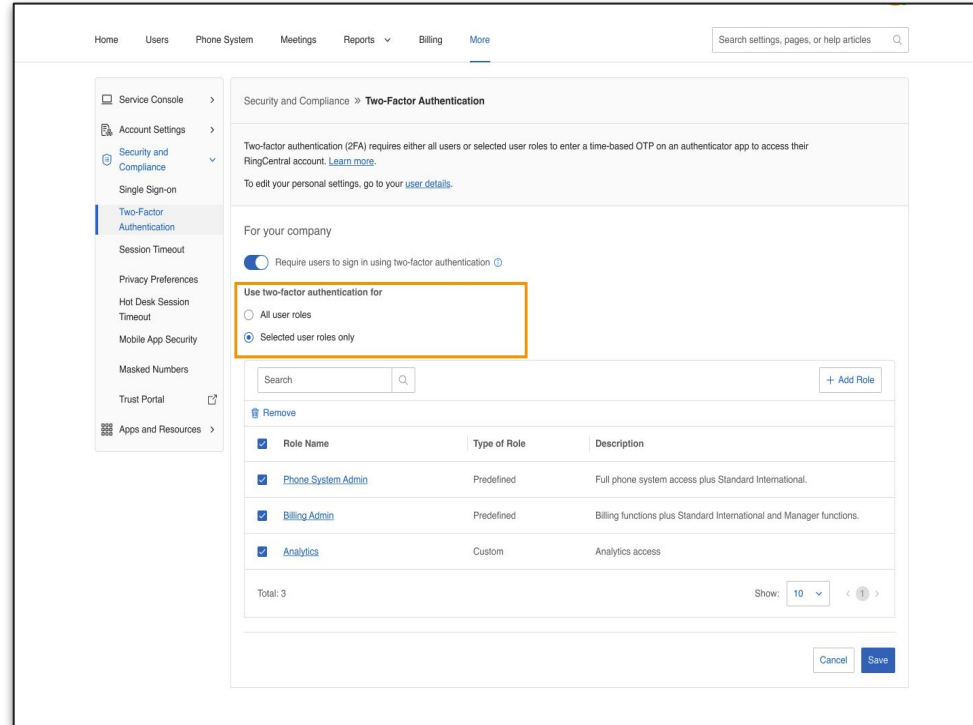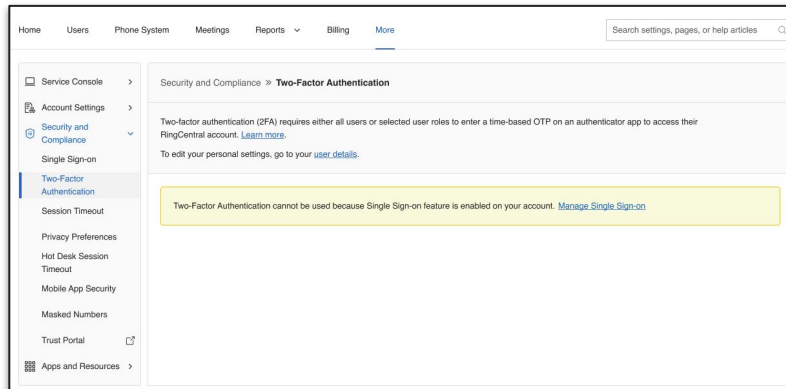
Feature: *Update SW UI for Change Password, PIN, and Security Question*

What's new	• This feature improves the discoverability of resetting password, PIN, and security question, and better tailors UI messaging to the selected flow.
What problem does it solve	• There was no information or labeling in the UI for where to update the security question. Messaging within the app led users to believe they had to reset their password in order to update their security question.
Rollout plan	• GA in ~~24.4.2 minor~~ Moved to 25.1 • This feature is available to all brands

Feature: *Update SW UI for Change Password, PIN, and Security Question*

How it works:
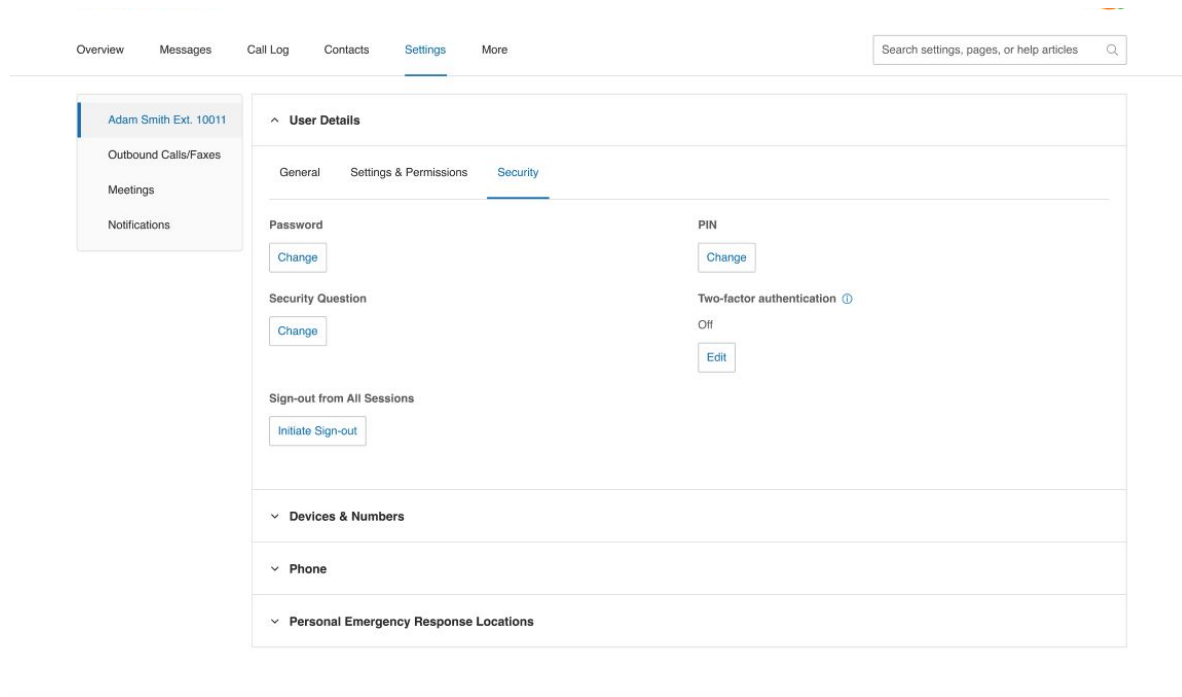
Password, PIN, and Security Question settings are now visually separated in the UI.

Feature: *Restrict Email Domain for Notifications & Other emails*

What's new	The ability to Restrict Email Domain for Notifications & Other emails

What problem does it solve	• As part of enterprise security requirements we have introduced a number of features to allow customers to restrict who may access their RingCentral Service. • This enhancement is also requested by FedRamp requirements to support restriction of notifications only to specific email domains.

Rollout plan	General Availability All Brands ~~24.4 minor,~~ moved to 25.1.2 Default **Enabled+off**

Feature: *Restrict Email Domain for Notifications & Other emails*

New configuration window will be present for Email Domain Restriction Configuration. This configuration window will be accessible with "AccountAdministration" permission.

Within the EDRC window the user will have an option to enter a list of Allowed Email Domains.

When the email will be sent out by the UNS only the emails with the Allowed Email Domain will be sent.

Feature: *Restrict Email Domain for Notifications & Other emails*

| Home | Users | Phone System | Reports ⌄ | Billing | More |

Security and Compliance 》 **Email Domain Restrictions**

Email domain restriction ensures that specific emails are only sent to addresses within a specified list of allowed domains.

- 🖥 Service Console ›
- ⚙ Account Settings ›
- ▤ **Security and Compliance** ⌄
- Single Sign-on
- Two-Factor Authentication
- Phone
- Session Timeout
- Privacy Preferences
- Hot Desk Session Timeout
- HIPAA Settings
- **Email Domain Restictions**
- Geo IP Restrictions
- Mobile App Security
- Masked Numbers & Location Data
- Trust Portal
- ⠿ Apps and Resources ›

🔵 Restrict email domains to a specified list

Allowed email domains

Specify domain names allowed to receive emails. Emails sent to addresses outside this list will be blocked.

Enter email domains ⓘ

[   ]   ＋ Add

Enter email domain ⓘ

Enter the domain part of the email address, like example.com. This is the part after the "@" symbol.

Save

Feature: *Restrict Email Domain for Notifications & Other emails*

Home   Users   Phone System   Reports ⌄   Billing   More

Security and Compliance   »   **Email Domain Restrictions**

Email domain restriction ensures that specific emails are only sent to addresses within a specified list of allowed domains

- Service Console →
- Account Settings →
- Security and Compliance ⌄
  - Single Sign-on
  - Two-Factor Authentication
  - Phone
  - Session Timeout
  - Privacy Preferences
  - Hot Desk Session Timeout
  - HIPAA Settings
  - Email Domain Restictions
  - Geo IP Restrictions
  - Mobile App Security
  - Masked Numbers & Location Data
  - Trust Portal
- Apps and Resources →

⬤ Restrict email domains to a specified list

Allowed email domains

Specify domain names allowed to receive emails. Emails sent to addresses outside this list will be blocked.

Enter email domains ⓘ

| energy.gov | + Add |

Enter email domains in FQDN format ⓘ

| gmail | + Add |

Please used standard email domain formats (eg. example.com)

Save

Feature: *Restrict Email Domain for Notifications & Other emails*

| Home | Users | Phone System | Reports ⌄ | Billing | More |

Service Console ›
Account Settings ›
Security and Compliance ⌄
Single Sign-on
Two-Factor Authentication
Phone
Session Timeout
Privacy Preferences
Hot Desk Session Timeout
HIPAA Settings
Email Domain Restictions
Geo IP Restrictions
Mobile App Security
Masked Numbers & Location Data
Trust Portal
Apps and Resources ›

Security and Compliance » **Email Domain Restrictions**

Email domain restriction ensures that specific emails are only sent to addresses within a specified list of allowed domains

🔵 Restrict email domains to a specified list

Allowed email domains

Specify domain names allowed to receive emails. Emails sent to addresses outside the approved list will be blocked.

Enter email domains ⓘ

[   ]   ＋ Add

Approved domains list	
energy.gov	Remove

Save

Feature: *Restrict Email Domain for Notifications & Other emails*

Home	Users	Phone System	Reports ⌄	Billing	More

☐ Service Console ⟩

⚙ Account Settings ⟩

▤ Security and Compliance ⌄

  Single Sign-on

  Two-Factor Authentication

  Phone

  Session Timeout

  Privacy Preferences

  Hot Desk Session Timeout

  HIPAA Settings

  Email Domain Restictions

  Geo IP Restrictions

  Mobile App Security

  Masked Numbers & Location Data

  Trust Portal

▦ Apps and Resources ⟩

Security and Compliance » **Email Domain Restrictions**

Email domain restriction ensures that specific emails are only sent to addresses within a specified list of allowed domains.

🔵 Restrict email domains to a specified list

Allowed email domains

Specify domain names allowed to receive emails. Emails sent to addresses outside the approved list will be blocked.

Enter email domains ⓘ

| [   ] | + Add |

Approved domains list	
energy.gov	Remove
treasury.gov	Remove
labor.gov	Remove

Save

Feature: *Restrict GeoIP/IP for App & Service Web*

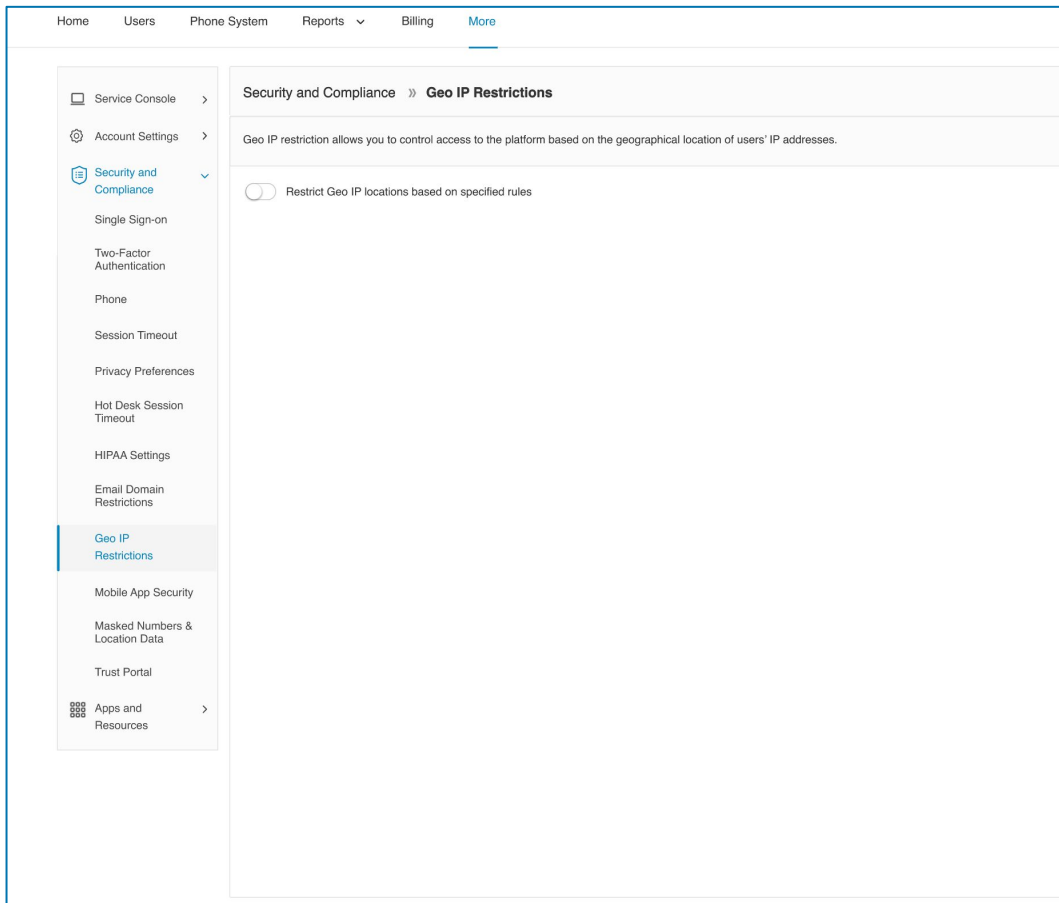| **What's new**	The ability to Restrict Apps and ServiceWeb based on their GeoIP/IP
What problem does it solve	Federal agencies have higher security demands compared to our usual SMB client base. While not explicit FedRAMP requirements Network Access controls are generally implemented for Gov Cloud customer networks. RingCentral does NOT have a similar control at the account level today. We DO allow this in a rough method at the partner level.
Rollout plan	General Availability All Brands 24.4 minor Enabled+off

New configuration window will be present for Geo IP Restriction Configuration. This configuration window will be accessible with "AccountAdministration" permission.

Within the GRC widows a user will be able to configure "Rules" using IP-Ranges and/or Countries and either explicitly allow or block them.

Feature: *Restrict GeoIP/IP for App & Service Web*

Home   Users   Phone System   Reports ⌄   Billing   More

Service Console   ›
Account Settings   ›
Security and Compliance   ⌄
    Single Sign-on
    Two-Factor Authentication
    Phone
    Session Timeout
    Privacy Preferences
    Hot Desk Session Timeout
    HIPAA Settings
    Email Domain Restrictions
    Geo IP Restrictions
    Mobile App Security
    Masked Numbers & Location Data
    Trust Portal
Apps and Resources   ›

Security and Compliance » **Geo IP Restrictions**

Geo IP restriction allows you to control access to the platform based on the geographical location of users' IP addresses.

🔵⬤ Restrict Geo IP locations based on specified rules

Geo IP Policy

Active Policy   Draft Policy

Add rules to specify countries or IP ranges which should be either blocked or granted access to the system. Rules will trigger in the order displayed.

Default if no other rule applies: Allow   ✎ Edit Draft   ⋮

Country / IP range	Description	Access control

You have no rules yet.

To begin restricting access from Geo IP locations,
add rules in your draft policy, and activate when ready.

Edit Draft

Feature: *Restrict GeoIP/IP for App & Service Web*

Add Geo IP Rule

Condition type

(•) Country   ( ) IP address / range

Country

| Select ⌄ |

Description

| Enter a short description, max 64 char. |

Access control

( ) Block   ( ) Allow

Cancel   Add

Feature: *Restrict GeoIP/IP for App & Service Web*

Add Geo IP Rule

Condition type

○ Country ● IP address / range

IP address ⓘ

Enter an IP address or range

Description

Enter a short description

Access control

○ Block ○ Allow

Cancel Add

IP address ⓘ

Enter an IP addr

Specify an IP address or range using one of the following formats:

· **Single IPv4:** e.g. "195.18.17.1"

· **Range of IPv4:** e.g. "195.18.17.1-195.18.17.255"

· **CIDR subnet IPv4:** e.g. "195.18.17.1/24"

Add Geo IP Rule

Condition type

○ Country ◉ IP address / range

IP address ⓘ

| 195.18.17.1 |

Description

| Suspicious activity detected |

Access control

◉ Block ○ Allow

Cancel **Add**

Feature: *Restrict GeoIP/IP for App & Service Web*

Home   Users   Phone System   Reports ⌄   Billing   More

Service Console >
Account Settings >
Security and Compliance ⌄
  Single Sign-on
  Two-Factor Authentication
  Phone
  Session Timeout
  Privacy Preferences
  Hot Desk Session Timeout
  HIPAA Settings
  Email Domain Restrictions
  Geo IP Restrictions
  Mobile App Security
  Masked Numbers & Location Data
  Trust Portal
Apps and Resources >

Security and Compliance » **Geo IP Restrictions**

Geo IP restriction allows you to control access to the platform based on the geographical location of users' IP addresses.

◉ Restrict Geo IP locations based on specified rules

Geo IP Policy

Active Policy   **Draft Policy**

Add rules to specify countries or IP ranges which should be either blocked or granted access to the system. Rules will trigger in the order displayed.

Default if no other rule applies: ○ Block   ◉ Allow   + Add Rule   ⋮

		Country / IP range	Description	Access control	
⠿	1	195.18.17.1	Suspicious activity detected	✕ Block	⋮

Copy Active Policy to Draft   🛡 Activate Draft

Feature: *Restrict GeoIP/IP for App & Service Web*
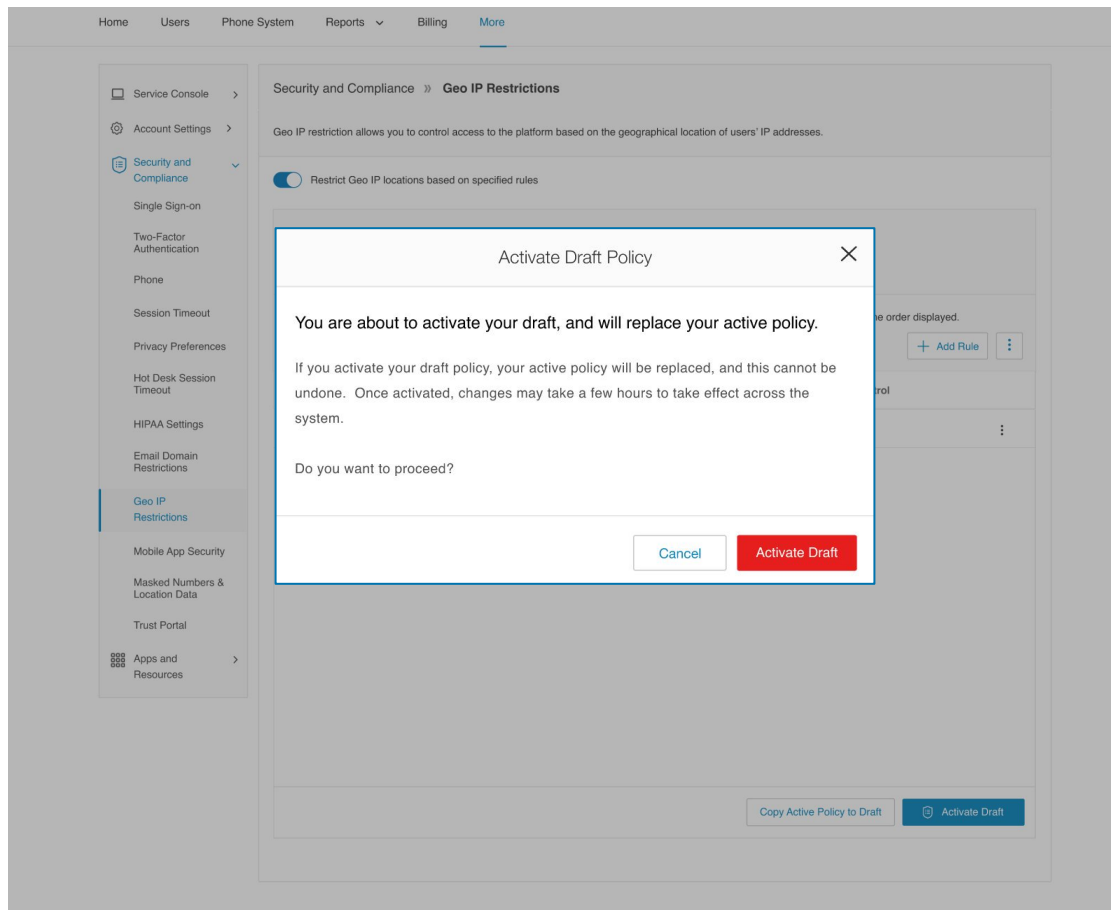
Feature: User-level toggle to restrict site numbers as caller ID

What's new	• This feature will allow admins to control their end users' use of their own site numbers as outbound caller ID
What problem does it solve	• From the Idea Community, some customers are looking to restrict their users' use of site numbers as outbound caller ID
Rollout plan	• GA 24.3.2 • This feature respects the multi-site SP, and is automatically enabled for all users when multi-site is enabled. This matches existing behavior to avoid disruption for existing customers.

How it works

In User Details, admins can restrict site numbers as caller id.

Feature: Delete User Flow: Reassign and Delete Numbers

| What's new	Introduce option for Re-assigning and Deleting Numbers for partner brands upon removing RingEX Extensions from the Admin Portal and in the App.
What problem does it solve	Partner-branded customers are not shown options to Reassign and Delete Numbers.
Rollout plan	• GA in 24.4 • All Partner Brands, All Packages • O@H 2.0 only

Feature: *Delete User Flow: Reassign and Delete Numbers*

How it works

RingCentral direct created a more optimized user deletion flow that streamlines the process. Today, in a partner brand, however, when users are deleted, the extension is automatically moved to an unassigned extension list instead of an option to present what to do with the number (whether to Move to Inventory, Reassign or Delete).

Before
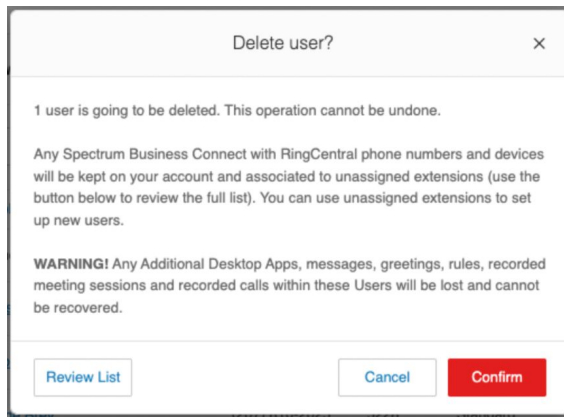
After
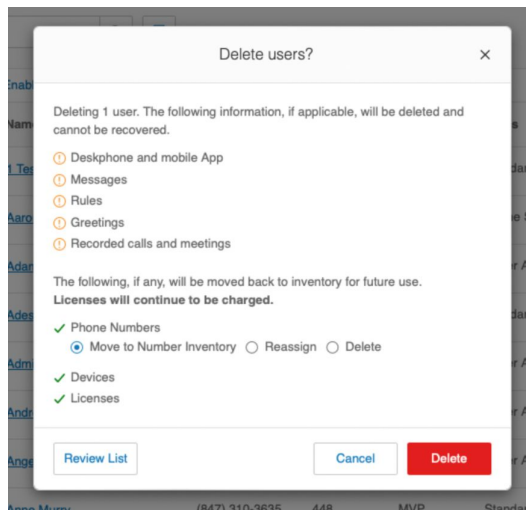
Admin Portal

In-App Onboarding Flow

Feature: *Delete User Flow: Reassign and Delete Numbers*
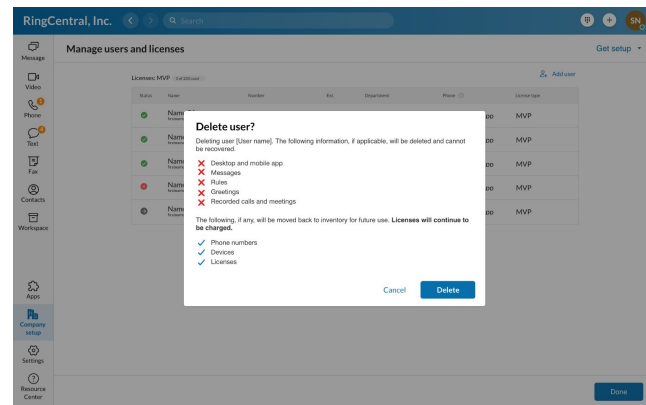
How it works

In-Life Purchasing. Some partner brands do not support In-Life Purchasing, so there are differences in the steps.

- ○ If brand supports In-Life Purchasing, Reassigning a number to a user will show a Billing Details form to purchase missing licenses (Single/Bulk).
- ○ If brand does NOT support In-Life Purchasing, a reminder will mention that operation cannot continue unless there are enough licenses in the account. If a license is available, it will use that license for the number reassignment

RC Number Management. If a partner manages their own phone numbers, there will also be a different set of behaviors

- ○ If numbers are managed by RC, "Delete" option will be shown to Agents and Users
- ○ If numbers are NOT managed by RC, "Delete" option will only be shown to Agents.

Feature: Purchase Type field rename for Device Information

What's new

Created a distinction between Purchased devices and Bring-your-own Devices (BYOD) across different fields in the Admin Portal (ServiceWeb) and SCP.

What problem does it solve

When users bring their own devices (BYOD) and add them to the system, Service Web and SCP is displaying devices that are either BYOD or Purchased as "Purchased" devices regardless, confusing the users on this device being a purchased one.

Rollout plan

- GA in 24.4
- All brands, all packages
- O@H 2.0 only

Feature: *Purchase Type field rename for Device Information*

How it works

ServiceWeb > Phone System > Device

When browsing into a specific device, the Purchase Type status will be shown here.

This is also applicable to Shared Lines

For Purchased devices, we won't show Equipment status.

Feature: *Purchase Type field rename for Device Information*

How it works

ServiceWeb > Billing > License and Inventory

There is now a distinction between BYOD and Purchased devices when viewing licenses and inventory.

How it works
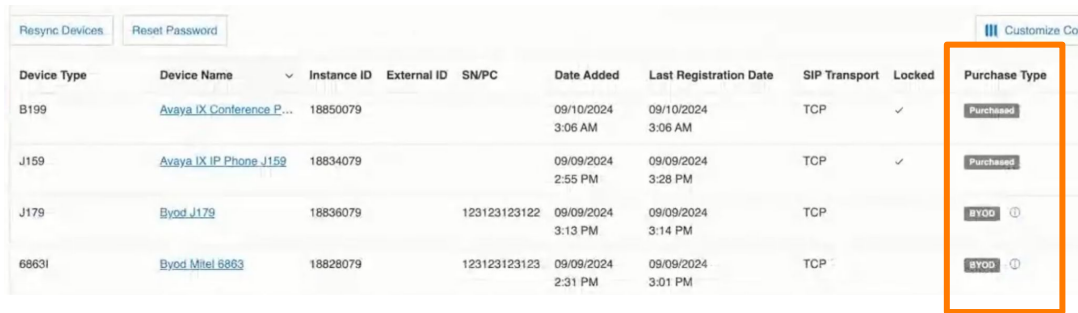
ServiceWeb > Billing > License and Inventory > Hardware

In the new License and Inventory UI, we will show filters for BYOD as well as the existing ones.
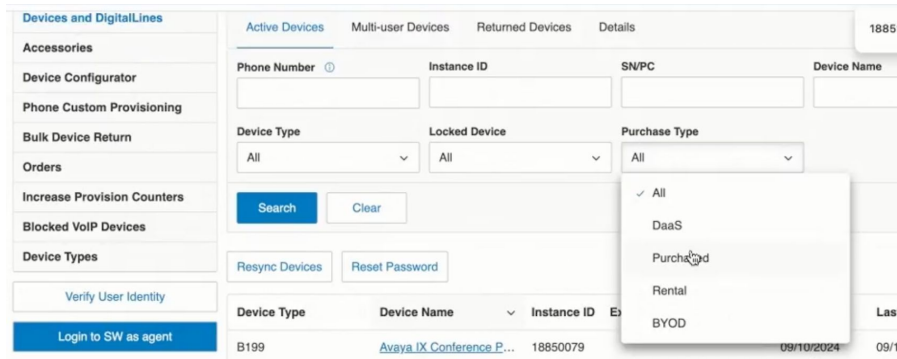
How it works

SCP > Accounts > Devices

Purchase Type now shown as either Purchased or BYOD.

For brands that support DaaS, it will show here as well.

SCP users can also filter Purchase Tpyes to BYOD to allow easier searching.

Feature: *Purchase Type field rename for Device Information*

How it works

SCP > Accounts > Devices

Call Handling

Feature: *Smart Automatic Call Recording Notifications*

What's new	• Smart Automatic Call Recording Notifications determines when to play a recording announcement based on the area code/number dialed.
What problem does it solve	• Today, recording notification announcements are always played regardless of the area code/number dialed.
Rollout plan	• GA: ~~24.4.2 minor~~ moved to 25.1 • Premium, Enterprise

Smart ACR Notification

- When automatic call recording notifications are turned ON, call participants hear a recording announcement notification when the call is connected.
"This call is being recording"

- If the call is unexpected, many callers will hang up not wishing to be recorded.

- Smart ACR disables recording for the call when two-party notification is required. The call is not recorded.

- This feature helps reduce the number of caller hang ups caused by unexpected recording notifications.

"This call is being recorded"

User dials
1-210-555-1212

What is this about?

"This call is being recorded"

PSTN
1-210-555-1212
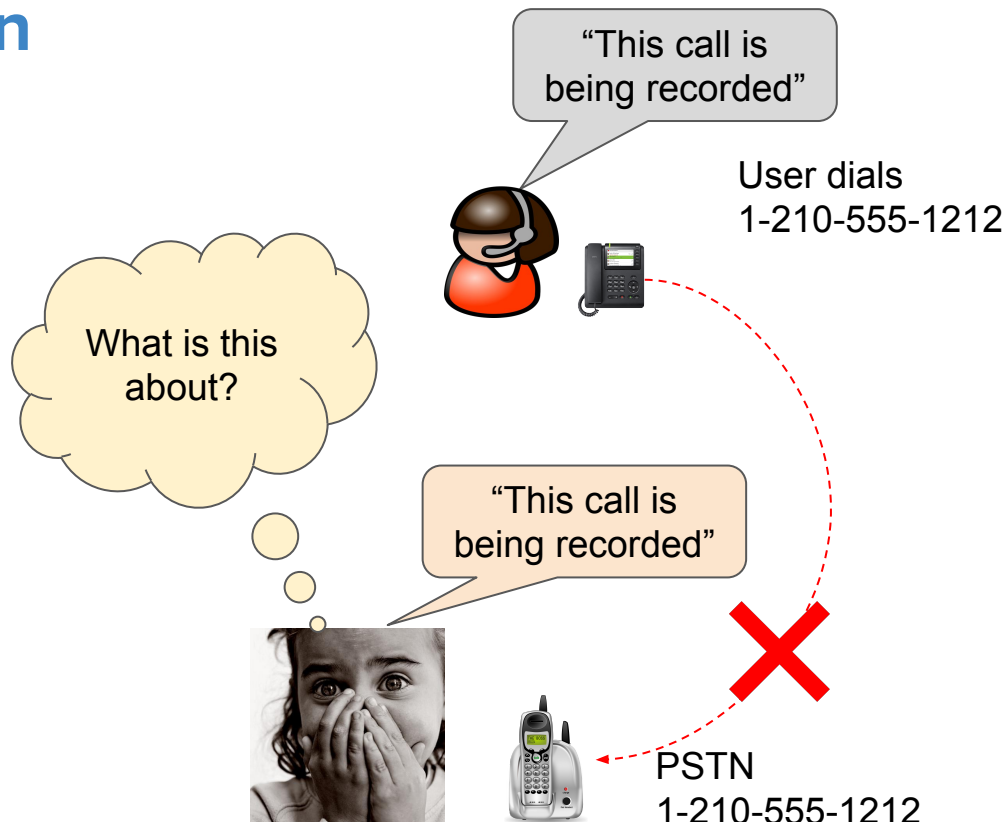
Smart ACR Notification

- When an outbound call is placed from a US DigitalLine to a US phone number with Smart ACR turned on, we lookup the call recording notification requirements based on the destination area code.

- If the destination area code resides in a State requiring one-party notification, the User (originating party) hears the recording announcement.

- If the destination area code resides in a State requiring two-party notification, call recording is disabled for the call and no recording announcement is played. The call is not recorded.

"This call is being recorded"

User dials
1-210-555-1212

PSTN
1-210-555-1212
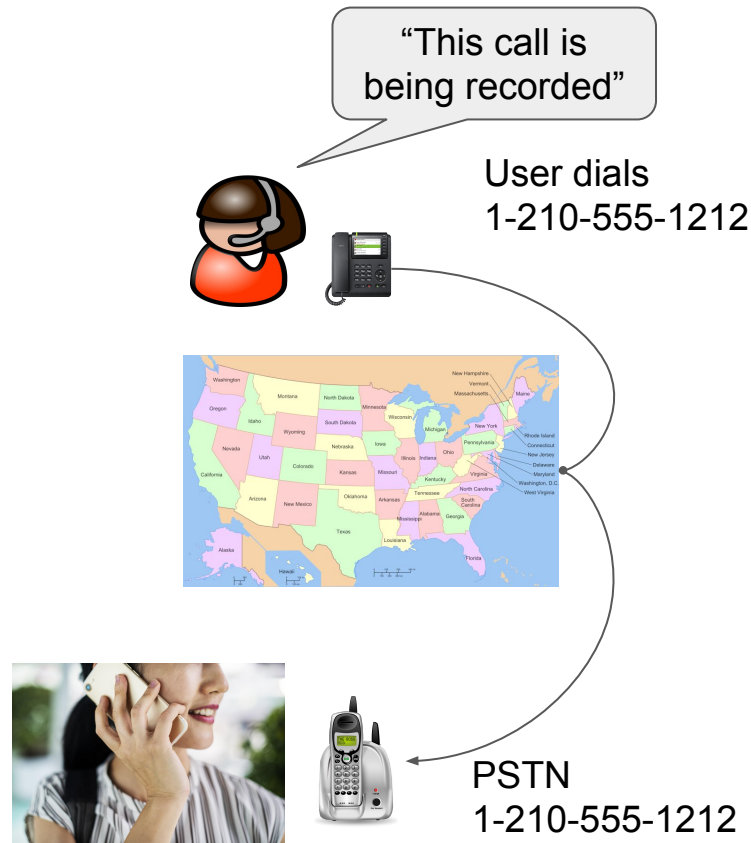
Smart Automatic Call Recording (ACR) Notification

- Call recording notification requirements vary by State.

- Smart ACR uses area codes to determine when a recording notification should be played to call participants during an outbound call.
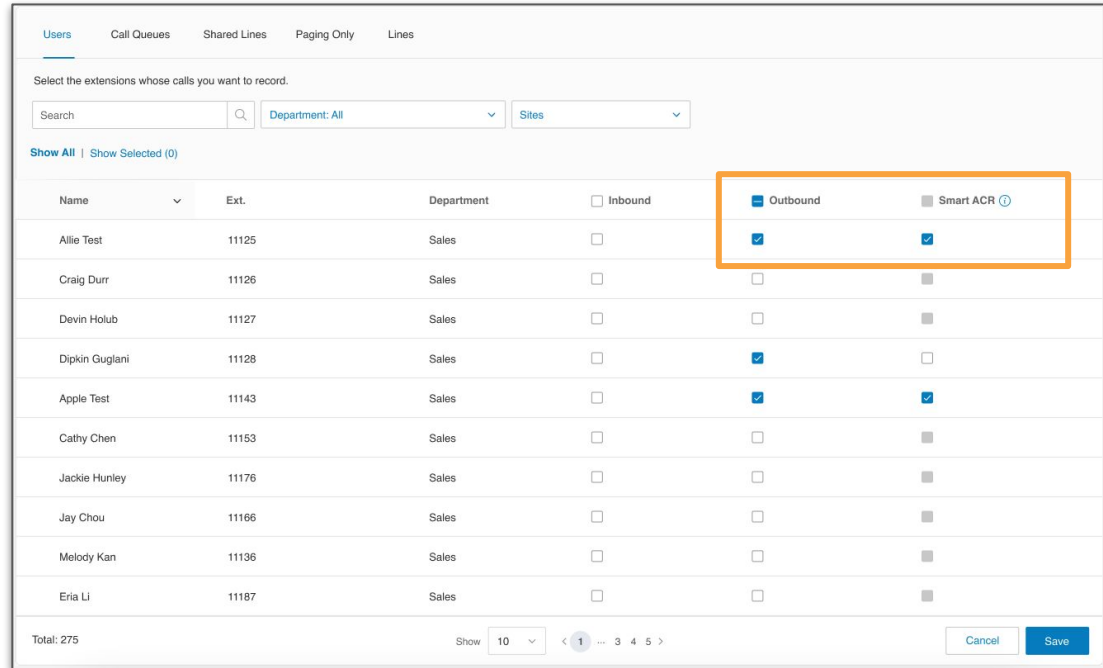
Smart ACR Notification

- Smart ACR only applies to outbound calls placed from US phone numbers.

- Smart ACR does not apply to inbound call recording nor outbound calls from non-US numbers.

- To turn on Smart ACR, first select Outbound recording for the desired users, then select Smart ACR.

One-party Recording Notification Area Codes

Recording announcement is played to person placing the outbound call (originating party)

State		Area Codes
Alabama	AL	205, 251, 256, 334, 659, 938
Alaska	AK	907
Arizona	AZ	480, 520, 602, 623, 928
Arkansas	AR	
Colorado	CO	303, 719, 720, 970, 983
Washington DC	DC	202, 771
Georgia	GA	229, 404, 470, 478, 678, 706, 762, 770, 912, 943
Hawaii	HI	808
Idaho	ID	208, 986
Indiana	IN	219, 260, 317, 463, 574, 765, 812, 930
Iowa	IA	319, 515, 563, 641, 712
Kansas	KS	316, 620, 785, 913
Kentucky	KY	270, 364, 502, 606, 859
Louisiana	LA	225, 318, 337, 504, 985

One-party Recording Notification Area Codes

Recording announcement is played to person placing the outbound call (originating party)

State		Area Codes
Maine	MA	207
Minnesota	MI	218, 320, 507, 612, 651, 763, 952
Mississippi	MS	228, 601, 662, 769
Missouri	MO	314, 417, 557, 573, 636, 660, 816
Nebraska	NE	308, 402, 531
New Jersey	NJ	201, 551, 609, 640, 732, 848, 856, 862, 908, 973
New Mexico	NM	505, 575
New York	NY	212, 315, 332, 347, 363, 516, 518, 585, 607, 631, 646, 680, 716, 718, 838, 845, 914, 917, 929, 934
North Carolina	NC	252, 336, 472, 704, 743, 828, 910, 919, 980, 984
North Dakota	ND	701
Ohio	OH	216, 220, 234, 326, 330, 380, 419, 440, 513, 567, 614, 740, 937
Oklahoma	OK	405, 539, 572, 580, 918
Oregon	OR	458, 503, 541, 971
Rhode Island	RI	401
South Carolina	SC	803, 839, 843, 854, 864
South Dakota	SD	605

One-party Recording Notification Area Codes

Recording announcement is played to person placing the outbound call (originating party)

State		Area Codes
Tennessee	TN	423, 615, 629, 731, 865, 901, 931
Texas	TX	210, 214, 254, 281, 325, 346, 361, 409, 430, 432, 469, 512, 682, 713, 726, 737, 806, 817, 830, 832, 903, 915, 936, 940, 945, 956, 972, 979
Utah	UT	385, 435, 801
Virginia	VA	276, 434, 540, 571, 703, 757, 804, 826, 948
Vermont	VT	802
West Virginia	WV	304, 681
Wisconsin	WI	262, 414, 534, 608, 715, 920
Wyoming	WY	307

Two-party Recording Notification Area Codes

Automatic recording is disabled for the call. The call is not recorded.

State		Area Codes
California	CA	209, 213, 279, 310, 323, 341, 350, 408, 415, 424, 442, 510, 530, 559, 562, 619, 626, 628, 650, 657, 661, 669, 707, 714, 747, 760, 805, 818, 820, 831, 840, 858, 909, 916, 925, 949, 951
Connecticut	CT	203, 475, 860, 959
Delaware	DE	302
Florida	FL	239, 305, 321, 352, 386, 407, 448, 561, 656, 689, 727, 754, 772, 786, 813, 850, 863, 904, 941, 954
Illinois	IL	217, 224, 309, 312, 331, 447, 464, 618, 630, 708, 773, 779, 815, 847, 872
Maryland	MD	240, 301, 410, 443, 667
Massachusetts	MA	339, 351, 413, 508, 617, 774, 781, 857, 978
Michigan	MI	231, 248, 269, 313, 517, 586, 616, 734, 810, 906, 947, 989
Montana	MT	406
Nevada	NV	702, 725, 775
New Hampshire	NH	603
Pennsylvania	PA	215, 223, 267, 272, 412, 445, 484, 570, 582, 610, 717, 724, 814, 835, 878
Washington	WA	206, 253, 360, 425, 509, 564

Smart ACR Feature Summary

	Call Recording	Outgoing Caller (RC User)	Called Party (PSTN) Area code in 1 party notification location e.g TX	Called Party (PSTN) Area code in 2 party notification location e.g CA
Smart ACR OFF	Active	Hears announcement	Hears announcement	Hears announcement
Smart ACR ON One-party notification location	Active	Hears announcement	No announcement	
Smart ACR ON Two-party notification location	Disabled	No announcement The call is not recorded.	-	No announcement The call is not recorded.

FAQ

Who defines the area codes that correspond to 1 party vs 2 party consent calling destinations?
- RingCentral defined the area codes.

Who can configure Smart ACR?
- Recording settings are configured by users with the Phone System - Auto-receptionist permission.

What types of calls are affected by Smart ACR?
- Smart ACR applies to outbound calls placed from US phone numbers to US phone numbers.

Does this feature affect all users on the account?
- Smart ACR is enabled on a per user/extension basis

Does this feature affect On-Demand Recording?
- No, On-Demand recording notifications are always played. Smart ACR only applies to automatic call recording.

What happens if an outbound call is placed to a toll-free number or new area code not listed?
- Call recording is disabled for the call and no recording announcement is played. The call is not recorded.

Feature: *Site Call Recording Settings*

What's new
- Some jurisdictions require different recording settings.
- This feature allows Automatic and On-Demand recording settings to be configured differently per site location

What problem does it solve
- Today all sites share the same Automatic and On-Demand recording settings

Rollout plan
- GA 24.4.2 minor
- Premium, Enterprise

Site Call Recording Settings

- Call recording regulations vary by geographic location.

- Site Call Recording Settings allows Administrators to configure recording availability, notifications, and periodic tones differently by Site.

- Take greater control of the caller experience by customizing the recording notifications and periodic tones callers will hear based on regulatory needs.

- Automatic Call Recording on/off toggle is available on the Main site.

  - Click Extensions to Record to select the users and calls to capture

Site Call Recording Settings

● To customize a site's recording settings from a Child site, select the option 'Use custom call recording settings'

Site Call Recording Settings include:
● On-Demand Recording On/Off
  ○ Announcement on Start
  ○ Announcement on Stop
● Automatic Call Recording
  ○ Play period tones for outbound calls
  ○ Play call recording announcement for outbound calls
  ○ Allow mute in auto call recording
  ○ Call recording announcement
  ○ Extensions to Record

Site Call Recording Settings

- When you change the site assigned to an extension, the extension inherits the new site's call recording settings.

- For example, if on-demand recording is turned Off for site 1 and On for site 2 and a User is moved from site 1 to site 2, they will be able to use on-demand recording.

Site Call Recording Settings
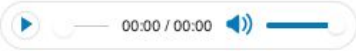
- Main site Administrators can check the option "Use Main site call recording settings for all sites" to lock Child Site recording settings so they cannot be changed individually.

Main Site (lock settings enabled)

Child Site (settings locked)

Feature: *Site and Call Queue call handling templates*

What's new	• Set custom rules for sites and call queues using templates

What problem does it solve	• Custom rules must be set for each site and call queue individually

Rollout plan	• 24.4.2 minor • All packages with calling capabilities.

Holiday and special event call routing for Sites and Call Queues made easy

- New call handling templates for Sites and Call Queues allow you to setup custom call rules in a single step.

- Easily change how calls are handled during company holidays, special events, or unexpected conditions.
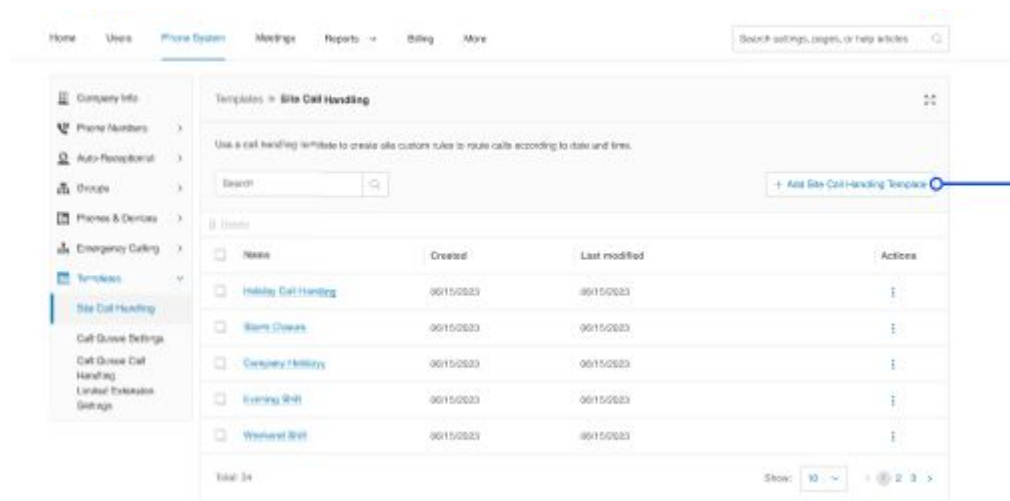
User Templates have been re-organized

- User templates have been re-organized.

- User templates include:
  - User Settings
  - User Call Handling
  - Key Templates

- Administrators with the User Management > Templates permission have access to User templ

User Roles
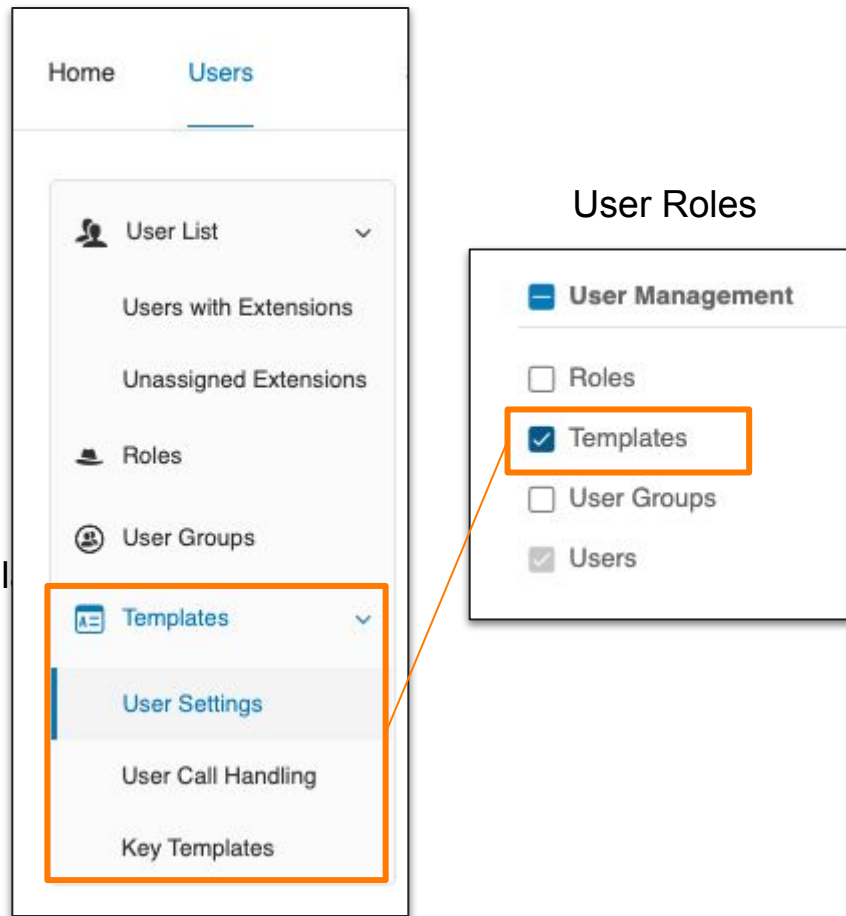
New Phone System templates

- Phone System templates include:
  - Site Call Handling
  - Call Queue Settings
  - Call Queue Call Handling
  - Limited Extension Settings

- Administrators with the Phone System > Templates > Sites permission have access to Site call handling templates.

- Administrators with the Phone System > Templates > Groups permission have access to Call Queue and Limited Extension templates.

Home	Users	Phone System

- Company Info ∨
  - Company Address
  - Caller ID Name
  - Directory Assistance
- Phone Numbers >
- Business SMS >
- Auto-Receptionist >
- Groups >
- Phones & Devices >
- Emergency Calling >
- Templates ∨
  - Call Queue Settings
  - **Call Queue Call Handling**
  - Limited Extension Settings
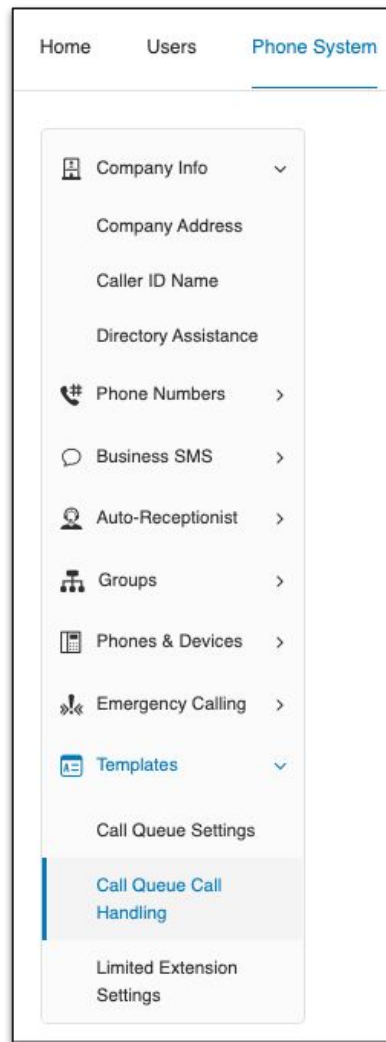
PLACEHOLDER for screen once Phone System > Templates permission is implemented

Date conditions for Site and Call queue call handling templates

- Site and Call queue call handling templates support two types of Date conditions.

- Select Weekly schedule to route calls during recurring events.

- Select Specific Date Range to route calls during non-recurring events such as holidays. Click + to add multiple dates.

Call routing for Site and Call queue call handling templates

- Site and Call queue call handling templates support multiple call routing options.

- You can send calls to voicemail, play an announcement, or forward calls to an extension or external number.

- Call queue templates also include the option to Ring call queue members.

Feature: Disable ability for Agents to turn off Accept Queue Calls toggle

What's new

- Context: On app's side, Accept Queue Calls toggle under profile controls if the call queue agent can receive calls from a call queue.
- New feature: Admins can configure which agents can have the ability to turn on/off Accept Queue Calls toggle.

What problem does it solve

- Today, call queue agents can toggle off "Accept Queue Calls" without reason, which brings up some problems like only one person is getting bombarded with calls or customers complaints their calls can not get through, which becoming management headache for customers(164 votes in idea portal).

Rollout plan

- 24.4.2 minor
- All brands

Feature: Enable delegated lines feature for partner brands

What's new
- This feature allows your primary number to appear on different phones or apps. With the delegated lines feature, you can: Call on behalf of, Hold and pick up within the group, Share lines or barge in. More feature
- No change to core feature capabilities, however SIP signalling enhancements also in scope to preserver PAI and History INFO for partner transport integration

What problem does it solve
- Close competitive gap between competition such as Cisco / BroadSoft
- Existing shared line and call delegation setups do not support the existing BCA requirements, making calls on the owners behalf, multiple appearances, and other requirements needed for existing customers

Rollout plan
- 24.3.2 Minor release
- Available for all packages (enabled on request SP1034 & SP1069)

1. Go to the Admin Portal and sign in.
2. Go to **Phone System > Groups > Delegated Lines**.
3. Click **New Delegated Line** at the upper right.

- Enter the Group Name, Manager's Email and Extension, then select the Number of Appearances.
- Click Next.
- Select an existing or add a new number for the owner and delegates to make and receive calls, then click Next.
- Click Add Owner to add an owner and device to the delegated line. If you already have existing owners, select from the list.
- Click Next.
- Enter the required information on the Select Delegates page and click Next.

Note: Each delegated line has one owner with one to 10 delegates. Each user can have multiple devices assigned, up to a max of 16 devices per line.

Integrations

Feature: SFDC Leave Conference as Host

What's new	Allow conference hosts to leave conference calls without hanging up the call

What problem does it solve	Currently conference hosts need to remain on the call in SFDC or the call will end for all parties

Rollout plan	Released to users on GA

Analytics

Feature: Business Analytics - Sharing a dashboard "As Is"

What's new	• New approach to share a dashboard "as I see it" or "using my permission level" (vs "using the viewers' permission level" or "as they allowed to see").

What problem does it solve	• It allows super admins to share a predefined dashboard exactly as an admin sees it. Normally, without this option, viewers will see only something that they're entitled to see. • This helps to share aggregated KPI dashboards to regional directors or analysts without adding those persons to multiple sites.

Rollout plan	• 24.3 minor

How it works

Business Analytics is controlled by three types of permissions.

User permissions
- Business Analytics is visible if a user has "Call Log - Site Access" - which can be visible for the whole company or be scoped to one site.

Data-level permissions

- Admin and super admins who can set company roles can view data for your organization's entire account.
- Admins whose roles let them access only a specific site will only be able to view Business Analytics data from that same site.
- Standard users (those who have no additional roles) will be able to view only their own data.
- Managers of user groups and queues will be able to view their personal data as well as the data for the group(s) and/or queue(s) they manage.

Bypass

Dashboard-level permissions
- Private/public/shared dashboard that respects the data-level permissions (see above). This is a default behavior and it allows you to create **template**-like dashboards.
- Private/public/shared dashboards without data-level permissions: "As I see it". This is an alternative to subscriptions and downloads.

The latter is a new behavior.

Add Widget

Dashboard Settings

NAME
US KPIs for Regional Director

Owner
Alex D (Don't Edit)

Select Privacy Settings
- Private 🔒 — visible only to me.
- Public 🌐 — visible to anyone who has an access to Business Analytics.
- ● Shared 👤 — visible to specific group of people.

USERS
Agent005 Regional Director - Share As Is test ✕

Dashboard data visibility
- ☐ Show dashboard data identical to my view.

By selecting this option, the users will see all data same as you even if they don't have permissions to see it. If not selected, the users will see data based on their role/permission.

Cancel   Save

Hardware

Feature: *Firmware updates*

What's new

Firmware updates for the following models:
- Poly Edge FW 8.2.2 for Edge series
- Yealink FW 124.86.25.6 for T34W

What problem does it solve

Firmware upgrade addresses security issues and fixes bugs while adding support for upcoming features.

Rollout plan

- Available for all brands

Feature: *Firmware updates*

Vendor	Model	Firmware version	Release Notes	Start firmware rollout *	Firmware rollout completed *
Yealink	T34W	124.86.25.6	[T3 firmware release notes](#)	Oct 17, 2024	Oct 23, 2024
Poly	Edge series	8.2.2	[8.2.2 release notes](#)	Oct 17, 2024	Oct 23, 2024

Thank you