cymbus

Next-Gen SIP Trunking

User Guide

July 2026

Table of Contents

Welcome **4**
Access the Voice Portal 4
Access the Portal with Single Sign-On 4
Access the Portal with Local Authorization 4
Language Setting 5
Change Session Language 5
Change Default Language 5
Manage SIP Trunks **7**
Details 7
Account Codes 9
Forward All 9
Overflow Routing 10
Inbound Failover Routing 11
Account Codes 12
How to Use Account Codes 12
Account Codes Settings 13
Default Settings 13
Call Types 14
Use Cases 14
Account Codes Setup 17
Enable Account Codes on Account 17
Account Settings 18
Enable Account Codes on SIP Trunk 20
Manage Account Codes 21
Add Account Code 21
Edit Account Code 22
Disable Account Codes 22
Custom Caller ID 23
Manage Numbers 23
Originating Numbers 23
Map Assignments 25
Edit an Assignment 26
Delete an Assignment 26
Trunk Groups 27
Shared vs Independent Settings 27
Add or Manage SIP Trunk Group 28
Group Name 28
Forward Settings 28
Overflow Routing 28
Inbound Failover Routing 29
SIP Trunks 30
Extension Dialing **32**
Assign Extensions to SIP Trunk 32

© 2026 Cymbus, Inc.

cymbus

Local Services **33**
Supported Dialing Patterns 33
Enable Local Services 33
Social & Public Services 35
Call History **37**
Apply Call Filters 38
Select Call Options 38
Block Number 39
Details 39
Export a Call History Report 39
Email a Call History Report 40
Download a Call History Report 40
Call History Report Fields 40
Analytics **47**
Inventory 47
Account Settings **48**
Emergency Notifications 48
Configure Emergency Notifications 49
Test Notifications 49
Emergency Notification Log 50
SSO Authentication 51
SSO Configurations 52
Exemptions 53
Manage Single Sign-On 55
Add SSO Configuration 55
Enable SSO Configuration 56
Switch SSO Configurations 57
Disable SSO Configuration 57
Customer Notification Templates 57

© 2026 Cymbus, Inc.

Welcome to SIP Trunking

SIP, or Session Initiation Protocol, has become the standard voice connection method in the VoIP industry. A SIP trunk is a connection that carries calls for multiple endpoints, as opposed to most other SIP devices which carry calls for only a single endpoint. Trunks are usually connected to an on-premises PBX (private branch exchange) and are typically billed on a per-concurrent call basis in addition to any toll charges for calls placed across the trunk.

A SIP trunk can be set up to support any number of concurrent calls, or channels, but a specific trunk is limited to the concurrent call limit. Once that limit is reached, incoming calls follow the Overflow Routing settings. If a trunk fails, incoming calls follow the Inbound Failover Routing settings. Multiple SIP trunks allow for calls to failover to associated trunks seamlessly, allowing your service to continue if something happens to prevent calls in one office.

Access the Voice Portal

The Voice Portal is where you can manage the SIP trunks and settings on your account. To add a new SIP trunk, however, please contact Customer Support.

Access the Portal with Single Sign-On

Customer Support will have provided you with details on how to access the voice portal using the same credentials used for the other services they provide. You may be redirected to your portal via your telecom account or via a direct URL.

1. Go to https://user.cymbus.com/.
2. Click **[Sign in with SSO]**.
3. Enter your email.
4. Click **[Sign In]**.

For any issues accessing the portal, contact Customer Support.

Access the Portal with Local Authorization

When your account was created, you were sent an email that contains your login information. Keep that email safe so you can refer to it later. If you haven't received it, or if you don't have an email address on your account yet, please contact Customer Support.

1. Go to https://user.cymbus.com/.
2. Enter your username (not email) and password.
3. Check *Remember Me* if you want to save your username and password.
4. Click **[Login]**.

© 2026 Cymbus, Inc.

Password Requirements
Your password must be at least eight characters long and include at least one number and one special character, such as ^ $ * . [ ] { } ( ) ? " ! @ # % & / \ , > < ' : ; | _ ~ ` = + -. It cannot contain any part of your username.

Language Setting

Experience the voice platform in English, Canadian French, or Spanish, seamlessly integrated across audio prompts, system-generated emails, and more.

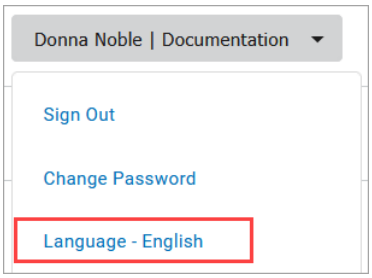
All users can change the language for their current session from the menu in the top right corner of the screen. Additionally, Admin end users can also set a default language for the account and each SIP trunk.

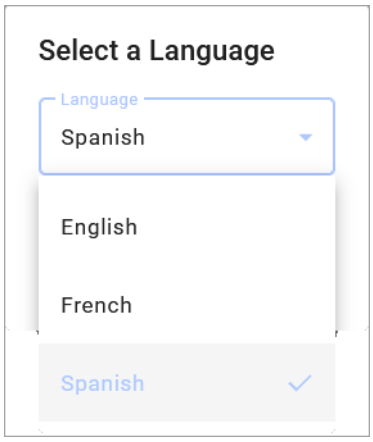
Change Session Language

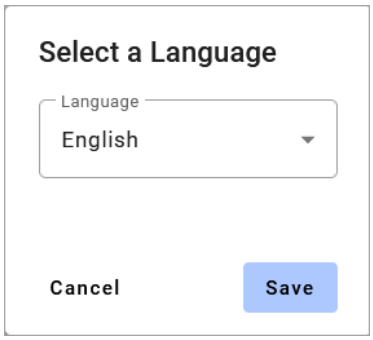
Follow the steps below to change the language used in the web portal for your active session:

1. Log in to the Voice Portal.
2. In the top right corner of the page, expand the menu with your name and select **Language**.
3. Choose a language: English, French, or Spanish.
4. Click **[Save]**. The portal will refresh to update with the selected language.

The portal will revert to your default language once you log out.







Change Default Language

A language can be set in the following locations:

- **Account.** The language setting assigned to the account applies to all users by default.

© 2026 Cymbus, Inc.

- **Account Managers.** The user's language setting applies to the web portal, IP phone (if the phone supports the language), telephone user interface (TUI) audio prompts, and system-generated emails. It does not affect the user's voicemail box, which is configured separately.

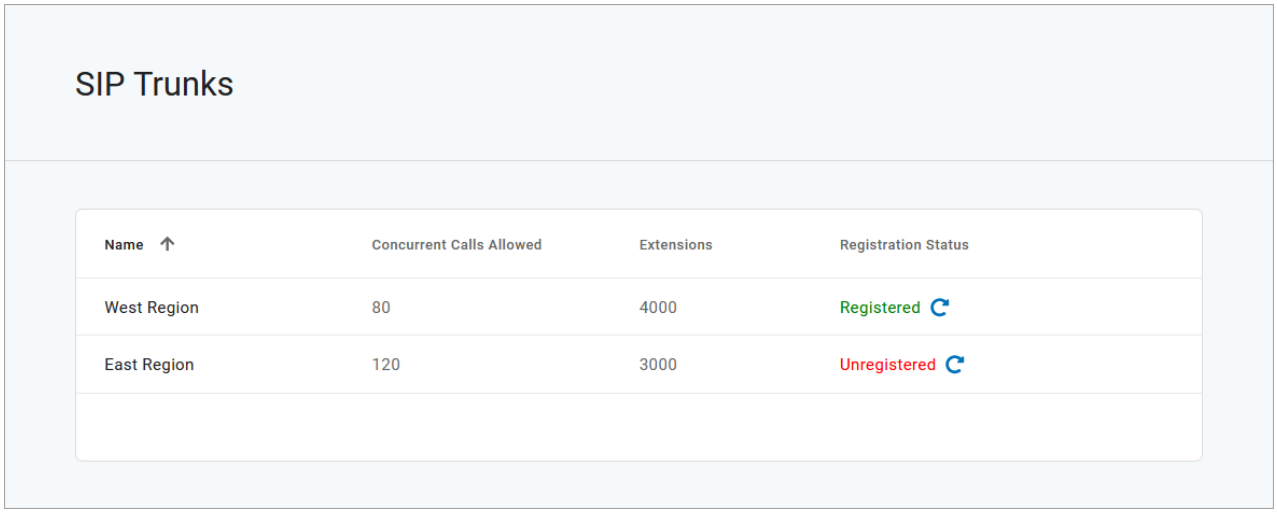
- **SIP Trunk.** The language setting on a SIP trunk applies to the telephone user interface (TUI) audio prompts. It does not affect the language used in the portal. See Manage SIP Trunks.

© 2026 Cymbus, Inc.

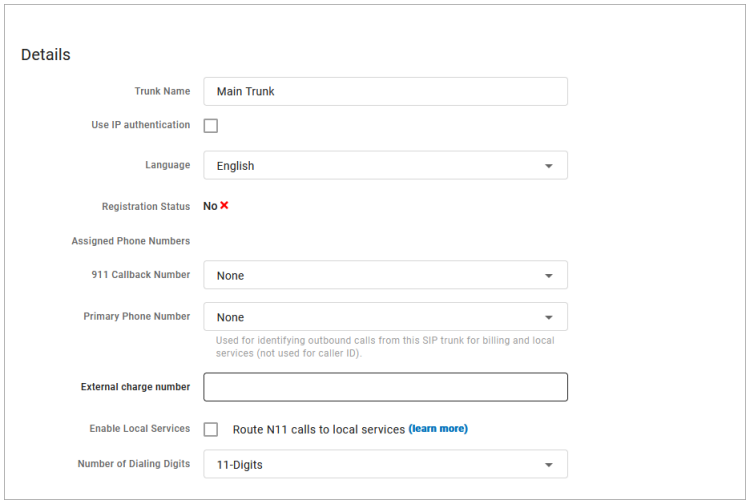
Manage SIP Trunks

To manage your SIP trunks, log in to the Admin Portal and go to **Account > SIP Trunk**. From here, select an existing trunk to view or modify the settings.

Here you can configure the SIP trunk settings, including forwarding, overflow and failover routing, concurrent call limits, and calling plans.



Details



Field	Description
Trunk Name	The name of the given SIP trunk.

© 2026 Cymbus, Inc.

Field	Description
Use IP authentication	Identifies whether this SIP trunk uses IP authentication. If unchecked, the trunk will authenticate via user-based SIP credentials, which will be provided in the *Authentication Credentials* section below (once the trunk is saved).
Language	Select a language for the trunk, which will be used for audio prompts: • English • French (Canadian) • Spanish
Registration Status	SIP trunk is connected to the platform and able to send and receive calls.
Assigned Phone Numbers	Lists every phone number with its destination set as this SIP trunk.
911 Callback Number	The phone number and address that emergency services will be given when a call comes in from the given SIP trunk. All phone numbers that call emergency services via this SIP trunk will have this phone number and address. Only one phone number and address can be assigned to a given SIP trunk.
Primary Phone Number	Select the phone number which will be used to identify outbound calls from this SIP trunk for local services (not for caller ID) and to determine any calling charges.
External Charge Number	A custom alphanumeric tag, such as an account name/number or phone number, which is added to the P-Charge-Info header for every outbound call from this trunk. This allows external billing systems to attribute calls to the correct account, regardless of the caller ID configured for the SIP trunk. If this field is not displayed and you have multiple carriers, talk to your Customer Success Manager.
Enable Local Services	Choose whether to enable local services dialing. Once enabled, the voice server will accept and route 3-digit N11 service numbers (411, 611, etc.) and 7-digit local dialing numbers from the SIP trunk. See Local Services for details.

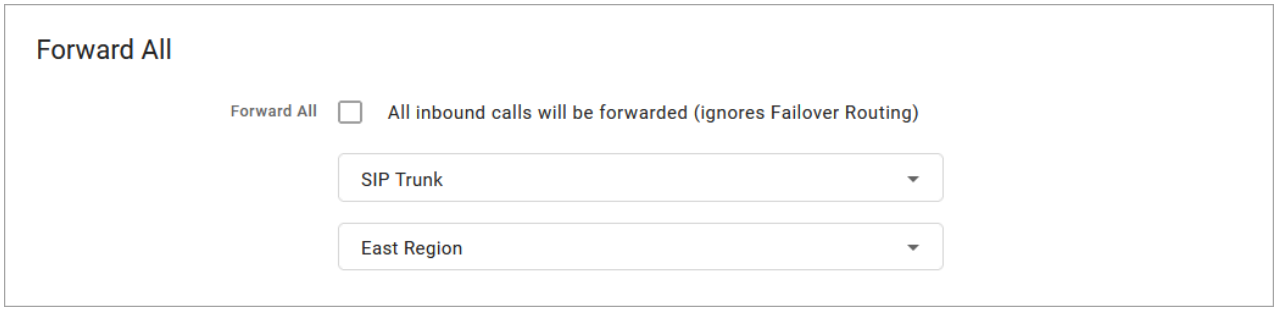
© 2026 Cymbus, Inc.

Field	Description
Number of Dialing Digits	Select the number of digits the SIP trunk will receive for inbound calls: • 7-digits: 123-4567 • 10-digits: 801-123-4567 • 11-digits: 1-801-123-4567

Account Codes

If Account Codes is enabled for the account, check this box to enable it on the SIP trunk.

Forward All



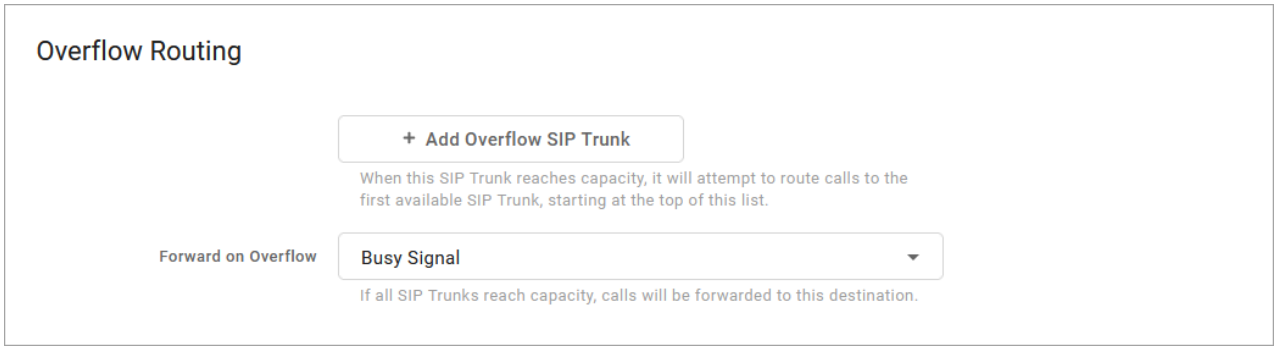
© 2026 Cymbus, Inc.

Field	Description
Forward All Calls	Check this box to forward all inbound calls intended for this SIP trunk to a specific destination: • SIP Trunk • User • Auto-Attendant • Voicemail • Telephone Number • Busy Signal

Overflow Routing

When the calls to the SIP trunk reach capacity (it has as many calls as allowed by the concurrent call setting on the SIP trunk), the Alianza platform will attempt to route calls according to this configuration. It will try these items in priority order. Multiple SIP trunks can be tried along with finally routing to another destination if all the attempts to route to configured SIP trunks fail.

In capacity exceeded scenarios, calls being routed to other SIP trunks will **not** follow the other SIP trunk's failover routing configuration.



Field	Description
[+ Add Overflow SIP Trunks]	Creates a new menu to select which SIP trunk calls will failover to.

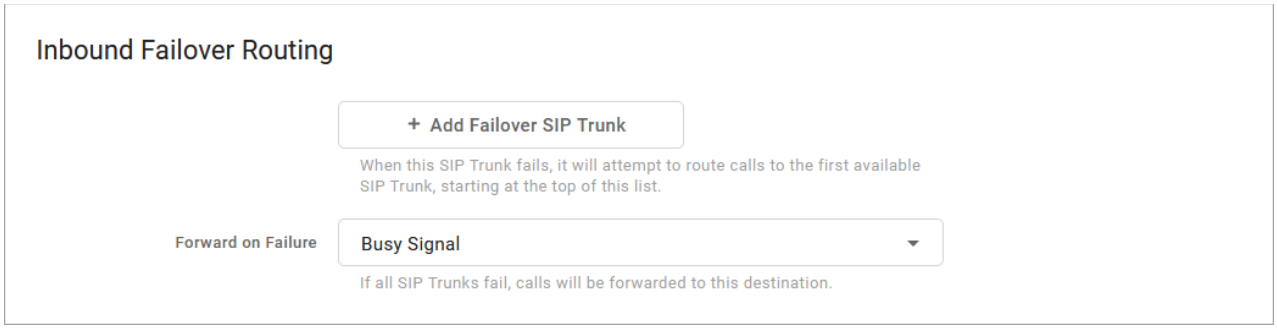
© 2026 Cymbus, Inc.

Field	Description
Forward on Overflow	If all SIP trunks reach the concurrent call limit, calls will be forwarded to the configured destination: • User • IVR • Voicemail • Telephone Number • Busy Signal

Inbound Failover Routing

When the calls to the SIP trunk fail, the Alianza platform will attempt to route calls according to this configuration. It will try these items in priority order. Multiple SIP trunks can be tried along with finally routing to another destination if all the attempts to route to configured SIP trunks fail.

In failover scenarios, calls being routed to other SIP trunks will **not** follow the other SIP trunk's failover routing configuration.



Field	Description
[+ Add Failover SIP Trunks]	Creates a new menu to select which SIP trunk calls will fail over to.

© 2026 Cymbus, Inc.

Field	Description
Forward on Failure	If all SIP trunks fail, calls will be forwarded to the configured destination: • User • IVR • Voicemail • Telephone Number • Busy Signal

Account Codes

Account Codes, also known as authorization codes, are used to tag (classify) calls for billing and reporting purposes and/or require authorization for calls to international locations, directory assistance, and premium toll numbers.

Admin users will create specific codes that end users can dial to associate call activity with a department, project, client account, and more. For example, if an agency needs to keep track of billable client calls, they can dial the code that corresponds to the client, and the code will be tagged in the Call History record. Later, the billing department can review the call records and bill each client appropriately.

Additionally, if an organization wants to require authorization for international calls, they can create codes for each user, then configure the account to require a valid account code for international calls. When a caller places a call to a country code that is different from their own, they will be asked to enter their code to authorize the call.

For additional use cases and how to set them up, see Account Codes Settings.

How to Use Account Codes

The general flow for using an account code on inbound and outbound calls is outlined below. However, it will change depending on which settings are enabled and disabled. See Account Codes Settings for details.

- **Outbound Calls:** Dial a phone number. When prompted, enter an account code (for example, 123).
- **Inbound Calls:** Answer an inbound call, then dial the star code + the account code (for example, *50123). The other party can hear the dial tones, so let them know what you're doing first.

See Account Codes Setup to enable it for the account and configure the default settings.

© 2026 Cymbus, Inc.

Mid-Call Star Code
If you don't know which star code is assigned to Account Codes, ask Customer Support. The star code allows users to tag inbound calls or outbound calls that don't require an account code.

Account Codes Settings

Account Codes settings can be configured for a variety of use cases. The default settings determine if codes are optional (used for tracking) or required (used for authorization), and the second group of settings determine what type of calls require them.

These settings are configured at the account level. See Account Codes Setup for details.

Default Settings

Require Account Codes for Internal Calls

If this setting is enabled, users are prompted to dial an account code on every outbound call that originates and terminates on this account.

- **On (Required):** The user dials an on-net phone number or extension and hears, *"Please enter a valid account code."*
- **Off (Optional):** The user dials an on-net phone number or extension. If they want to tag the call, the user can dial the star code + account code once the call is answered.

Validate Account Codes When Dialed

If this setting is enabled, outbound calls are not connected unless the caller enters a valid code. However, an inbound call will continue even if an incorrect code is entered to the max retry limit.

- **On (Validated):** The account code is checked against the codes on the account. Outbound calls are not connected unless the caller enters a valid code. Inbound calls, however, will continue even if the user enters invalid codes up to the max retry limit.
    - If the code is valid, the user hears a splash tone to indicate the account code was accepted. The call continues and the code is added to the Call History record.
    - If the code is not valid, the user hears, *"Invalid entry. Please enter an X-digit account code."*
- **Off (Not Validated):** The user can enter any code they want as long as it's the right length.
    - If the code is valid, the user hears a splash tone to indicate the account code was accepted. The call continues and the code is added to the Call History record.
    - If the code is too long or too short, the caller hears, *"Account codes must be X digits. Please re-enter your X-digit account code."*

© 2026 Cymbus, Inc.

Allow Call to Proceed After Max Retries

The max retry limit is set in **Account Codes Settings**. Once the caller reaches this limit on an outbound call, they hear:

- **On (Allow):** *"You have reached the maximum number of attempts. No account code will be assigned to this call."* And the call continues without an account code.
- **Off:** *"You have reached the maximum number of attempts to enter a valid account code. Goodbye."* The call is disconnected.

Call Types

Choose which specific call types require an account code. These optional settings are typically used to ensure that only authorized personnel can place certain types of calls that may incur additional charges.

If one or more call types are enabled, only those call types require an account code. However, if no call types are enabled, all calls require an account code.

- **International.** Require a code to authorize calls to country codes that are different than the caller's. Since the US and Canada have the same country code, calls between the countries are not considered international.
- **Directory assistance.** Require a code to authorize calls to directory assistance (411 and 0).
- **Premium toll.** Require a code to authorize calls to 1-900 numbers.

Validation Setting

To prevent users from placing these call types without a valid code, ensure the *"Validate account codes when dialed"* setting is enabled; otherwise, the call will go through even if the number dialed doesn't match a code on the account.

Use Cases

Settings	Results
Account Codes is not yet live. • Account Codes is enabled for the account. • Account Codes is not enabled for the SIP trunk.	• Account codes are not prompted for outbound calls. • Account codes are not allowed for inbound calls.

© 2026 Cymbus, Inc.

Settings	Results
Account codes are optional. • Account Codes is enabled for the account and SIP trunk. • Require account codes for internal calls: OFF • Calls requiring account codes: OFF	• Account codes are not prompted for calls that originate and terminate on the same account (internal calls). • Account codes are prompted for outbound calls to the PSTN. • Account codes are allowed for inbound internal calls.
Account codes are required. • Account Codes is enabled for the account and SIP trunk. • Require account codes for internal calls: OFF • Validate account codes when dialed: ON • Calls requiring account codes: OFF	• Account codes are prompted for outbound calls to the PSTN. • Account codes are not prompted for calls that originate and terminate on the same account (internal calls). • Account codes are allowed for inbound internal calls. • A valid account code is required. If the code dialed is invalid, the call will not proceed.
Track internal calls only. • Account Codes is enabled for the account and SIP trunk. • Validate account codes when dialed: OFF • Require account codes for internal calls: ON • Calls requiring account codes: OFF	• Account codes are prompted for outbound calls to the PSTN. • Account codes are not prompted for calls that originate and terminate on the same account (internal calls). • The account code dialed can be any number, so long as it is the correct length. • Account codes are allowed for inbound calls.

© 2026 Cymbus, Inc.

Settings	Results
Track all outbound calls. • Account Codes is enabled for the account and SIP trunk. • Validate account codes when dialed: OFF • Require account codes for internal calls: OFF • Calls requiring account codes: OFF	• Account codes are prompted for all outbound calls. • Account codes are allowed for inbound calls. • The account code dialed can be any number, so long as it is the correct length.
Require authorization for all outbound calls. • Account Codes is enabled for the account and SIP trunk. • Validate account codes when dialed: ON • Calls requiring account codes: OFF	• Account codes are prompted for all outbound calls. • Account codes are allowed for inbound calls. • A valid account code is required. If the code dialed is invalid, the call will not proceed.

Require authorization for international calls.
• Account Codes is enabled for the account and SIP trunk.
• Validate account codes when dialed: ON
• Calls requiring account codes:
  • International: ON
  • Directory assistance: OFF
  • Premium toll: OFF
	• A valid account code is required to place a call to international locations. If the dialed code is invalid, the call will not proceed.
	• All other calls are *not* prompted for an account code.
	• Account codes are allowed for inbound calls.

© 2026 Cymbus, Inc.

Settings	Results

Require authorization for calls to 1-900 numbers.
• Account Codes is enabled for the account and SIP trunk.
• Require account codes for internal calls: OFF
• Validate account codes when dialed: ON
• Calls requiring account codes:
  • International: ON
  • Directory assistance: ON
  • Premium toll: ON
	• Account codes are not prompted for outbound calls to the PSTN.
	• Account codes are not prompted for calls that originate and terminate on the same account (internal calls).
	• A valid account code is required to place a call to an international location, directory assistance, or a premium toll number.
	• Calls to local and national long-distance numbers are *not* prompted for an account code.

Account Codes Setup

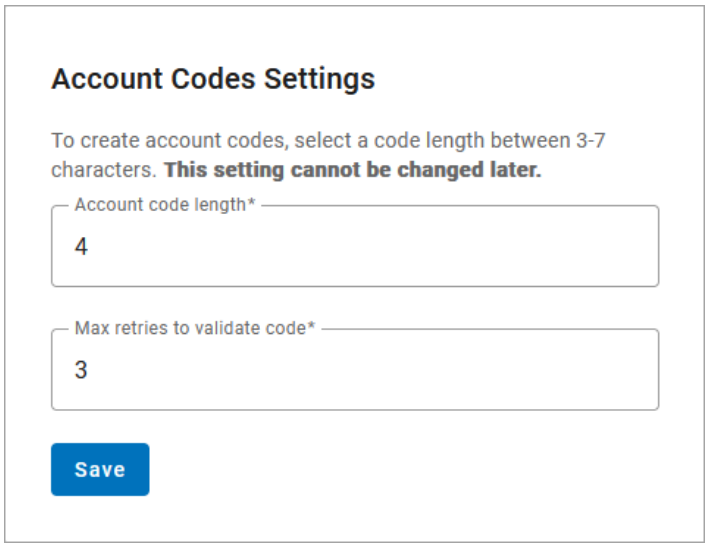
Account Codes settings are managed at the account level. Once it's enabled on the account and the default settings are configured, you can choose whether to enable Account Codes for all (current) SIP trunks, after which it can be enabled or disabled for individual trunks as needed.

Enable Account Codes on Account

The following steps are only required the very first time Account Codes is enabled on an account:

1. Go to the **Account Codes** page.
2. Fill out the following fields:
   - **Account code length:** Specify the number of digits (3–7) that will be required for all codes on this account. This setting cannot be changed later, so choose a length that will meet the account's needs in the long term.
   - **Max retries to validate code:** Specify how many times (1–9) a user can enter an incorrect account code. The industry average is 3–5 attempts.
3. Click **[Save]**. The page is refreshed, and Account Codes can now be configured on the account.

© 2026 Cymbus, Inc.



Account Settings

Once Account Codes is enabled on an account, the account-level settings must be configured before enabling it on SIP trunks. These settings are applied to all users who have account codes enabled, except those with custom settings.

Account Codes work differently depending on the settings. For details about how to configure your settings for different use cases, see Account Codes Settings.

1. Go to **Account > Account Codes**.
2. Under **Account Codes Settings**, switch on *Allow account codes*.
3. **Settings.** Choose which settings to enable (optional). To see how each of these settings changes the flow of a call, see Account Codes Settings.
    - **Require account codes for internal calls.** If enabled, users are prompted to dial an account code on every outbound call to other users on the account. If disabled, the user can dial a star code + account code during a call if they want to tag it.
    - **Validate account codes when dialed.** If enabled, the account code is validated against codes on the account. If disabled, the user can dial any number as an account code, as long as it's the right length. At least one account code must be added before enabling this option.
    - **Allow call to proceed after max retries.** If account codes are validated and the user enters multiple invalid codes, this setting determines whether the call will proceed as intended or end once the user reaches the max retry limit. This setting can only be customized at the user level if it's enabled at the account level first.
4. **Calls requiring account codes.** Choose which specific call types require an account code. These settings are typically used to ensure that only authorized personnel are able to place certain types of calls that may incur additional charges.

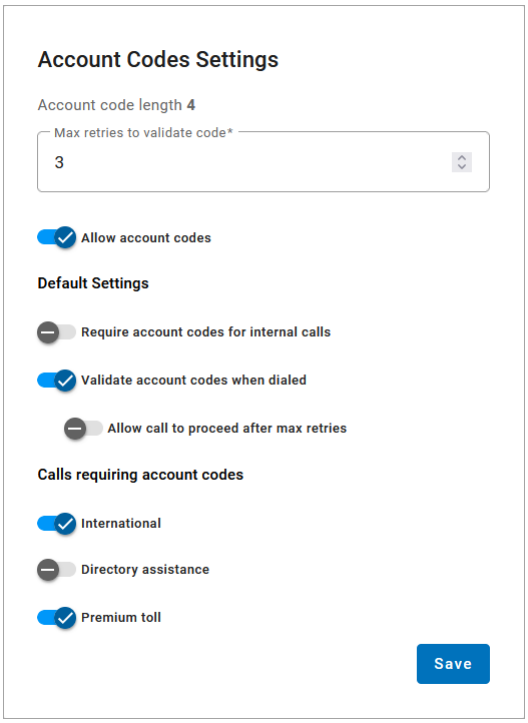
© 2026 Cymbus, Inc.

To prevent users from placing these call types without a valid code, ensure "Validate account codes when dialed" (above) is enabled. Otherwise, the call will go through even if the number dialed doesn't match a code on the account.

- **International.** Require a code to authorize calls to country codes that are different than the caller's. Since the US and Canada have the same country code, they're considered local.
- **Directory assistance.** Require a code to authorize calls to directory assistance (411) and operator assistance (0).
- **Premium toll.** Require a code to authorize calls to 1-900 numbers.

> **Important**
> If one or more call types are enabled, only those call types require an account code. However, if no call types are enabled, *all calls* require an account code.

5. Click **[Save]**.

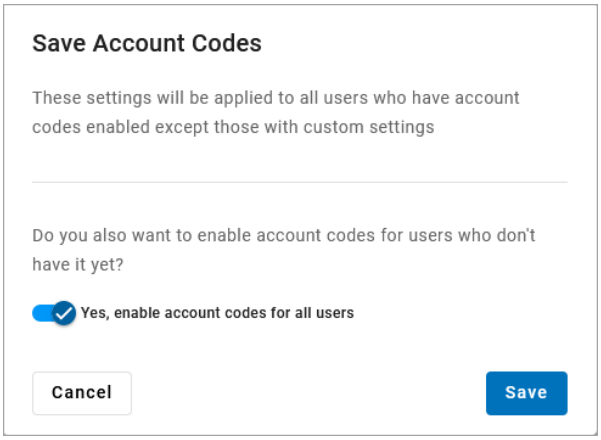


6. **Save Account Codes.** A pop-up will appear stating that these settings will be applied to all trunks that have account codes enabled, except those with custom settings, and ask if you want to enable this feature for all users who don't have it yet.
   - **Yes:** Account Codes will be enabled for all existing SIP trunks that don't have it yet. If Account Codes had been intentionally disabled for any SIP trunks, it will have to be disabled for them again.

© 2026 Cymbus, Inc.

- **No:** Account Codes will *not be* enabled for SIP trunks that don't have it yet. Choose this option if you want to enable it manually for individual trunks, rather than enabling it for all of them at once.

7. Click **[Save]** to apply the settings.



Enable Account Codes on SIP Trunk

The default settings configured at the account level apply to all SIP trunks that have Account Codes enabled. When Account Codes is enabled, callers are prompted to dial a code on every outbound call. Whether or not the code must be valid (preconfigured on the account) depends on the account's settings. See How to Use Account CodesHow to Use Account Codes for details.

When Account Codes is enabled for the account, it can automatically be enabled for all existing SIP trunks. However, it is *not automatically enabled* for new trunks, so it must be enabled manually for those that need it.

1. Go to the **SIP Trunks** page and select the trunk you want to customize.
2. Scroll down to **Account Codes**.
3. Check ***Enable account codes*** to turn it on. Once saved, callers will be prompted to dial an account code on every outbound call placed from the trunk.

4. Click **[Save]**. Account Codes is now enabled with the account settings.

Disable Account Codes
To disable Account Codes on a SIP trunk, uncheck *"Enable account codes"*. To disable the feature for the account (and all trunks), see Disable Account Codes

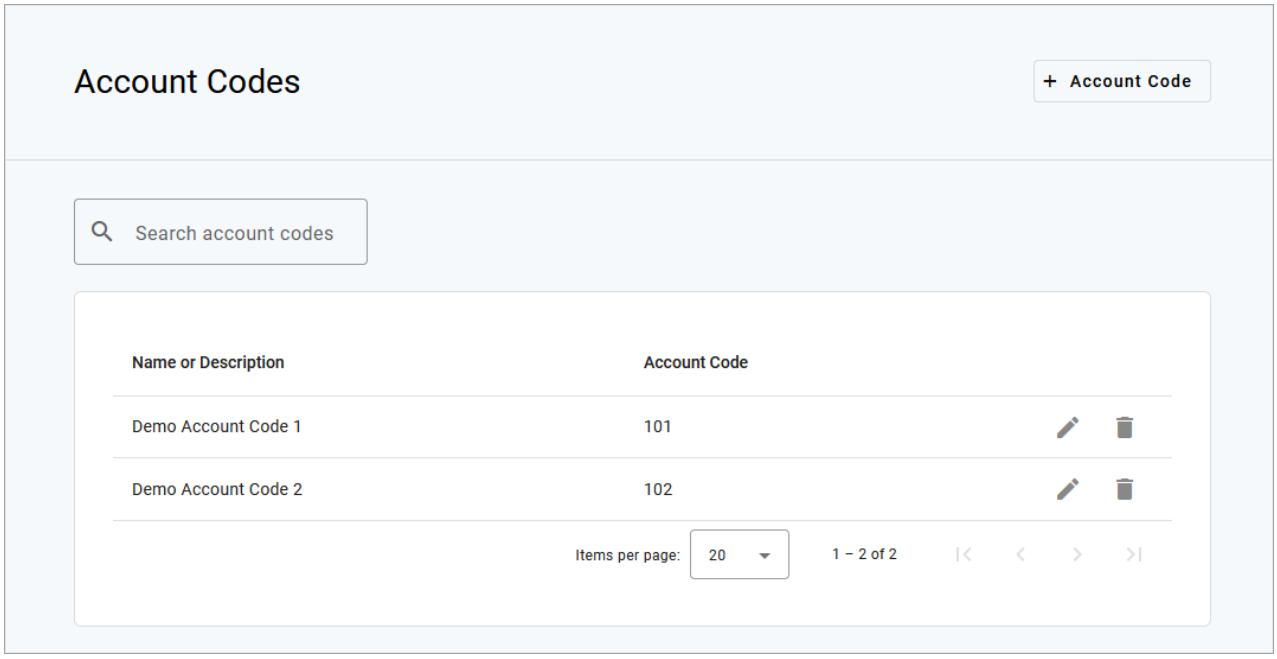
© 2026 Cymbus, Inc.

Manage Account Codes

Account Codes allow users to tag calls for billing purposes or authorize calls to international locations, directory assistance, or premium toll numbers. Create as many account codes as needed.

For calls that are prompted for an account code, if the "*Validate account codes when dialed*" setting is enabled, the user must dial a code that is set up on the account or the call will not proceed. However, if this setting is not enabled, the user can dial any code they want, whether or not it's set up on the account, as long as it's the right number of digits.

At least one code must be added to the account to enable this setting; otherwise, users won't be able to place outbound calls. Unless Account Codes are being used to authorize certain calls, we recommend creating at least one account code, such as 1000, that can be used as a default option.



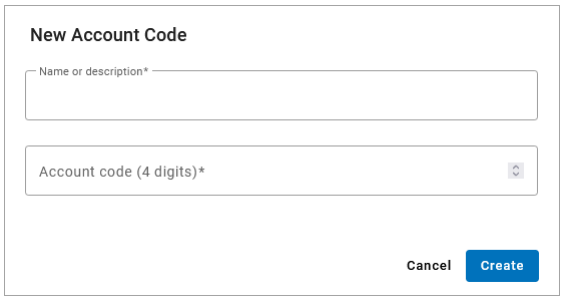
Important
Account codes cannot start with zero (0).

End User Access
End users don't have access to the list of account codes, so you'll need to provide them manually. Since codes cannot be assigned to specific users or for specific purposes, only give users the code(s) you want them to have.

Add Account Code

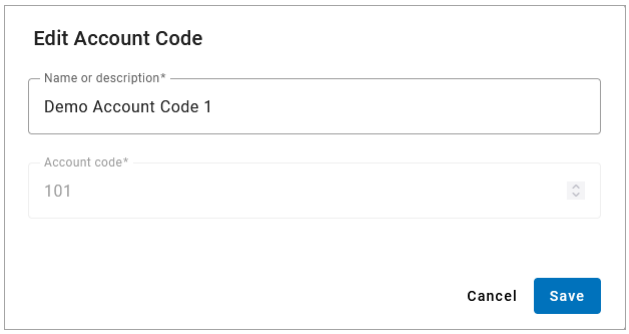
1. Go to the **Account Codes** page.

2. Click **[+ Account Code]** in the top right.
3. Enter a name or brief description to remember what the code is assigned for.
4. Enter the code that will be dialed.
5. Click **[Create].**
6. Repeat steps 2–5 for any additional codes.



Edit Account Code

Click the edit icon to update the name or description of an existing account code. To change the number, create a new one and then delete the old one.

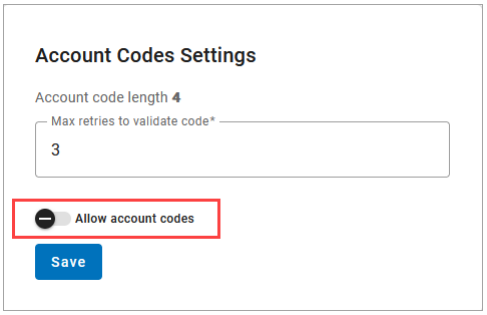


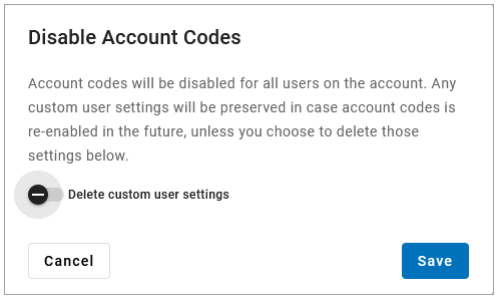
Disable Account Codes

When Account Codes is disabled at the account level, it is also disabled for all SIP trunks. To disable Account Codes for an individual SIP trunk, go to the trunk settings and uncheck *"Enable account codes"*. To disable it for the account, follow the steps below:

1. Go to the **Account Codes** page.
2. Under **Account Codes Settings**, toggle off *Allow account codes* and click **[Save]**.
3. Click **[Save]** to disable Account Codes for all SIP trunks on the account. The account codes are preserved, so they can be used again if the feature is re-enabled later.

© 2026 Cymbus, Inc.





Custom Caller ID

Custom Caller ID for SIP Trunking gives businesses the flexibility to display toll-free numbers, department-specific lines, or local presence numbers—regardless of the caller ID setting configured on their PBX—so callers see the right number for the right call.

To configure Custom Caller ID, service providers assign a pool of numbers to SIP trunks, add a set of custom caller ID phone numbers, then map each originating number to the right caller ID number. Alianza then inserts the custom caller ID number into the P-Asserted-Identity header on outbound calls while preserving the original FROM header, so the called party sees the custom caller ID number and not the number assigned by the PBX.

Interested?
Contact your Customer Success Manager to enable Custom Caller ID for SIP Trunking on your partition and let them know whether you'd also like to enable admin user access, which will allow Account Managers and Super Admin users to manage these settings in the end user portal.

Manage Numbers

Before caller ID can be customized, the originating phone numbers and caller ID phone numbers must be defined. The numbers added here are not verified, so double-check that the number entered is exactly what it should be.

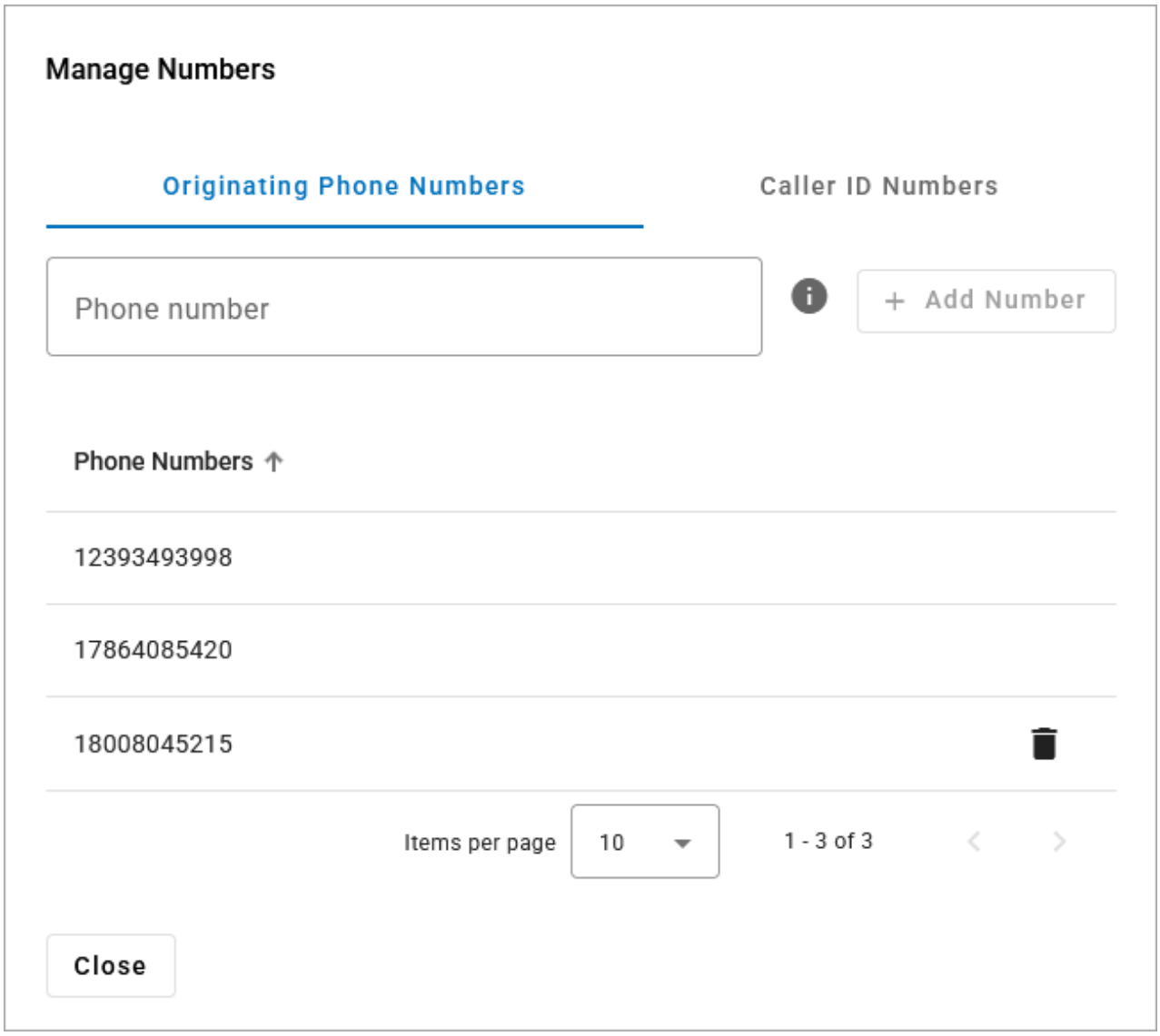
1. Go to **SIP Trunk > Custom Caller ID**.
2. In the right corner, select **[Manage Numbers]** to open the modal.

Originating Numbers

In the Manage Numbers modal, select the **Originating Phone Numbers** tab, phone numbers assigned to the SIP trunk are displayed below by default and cannot be removed. Enter any additional outbound phone numbers or wildcard ranges from your PBX in the *Phone number* field.

To remove an added number, select **Delete** on the right. If the number was assigned to a caller ID number, the assignment will also be deleted.

© 2026 Cymbus, Inc.



Wildcards

Wildcards can be used to indicate a range of originating numbers. To enter a wildcard range, enter the phone number and use an asterisk (*) to represent one or more missing digits. For example:

- * = Any phone number
- 801* or 1801* = Any number with the 801 area code
- 801555123***** = A range from 8015551230 to 8015551239

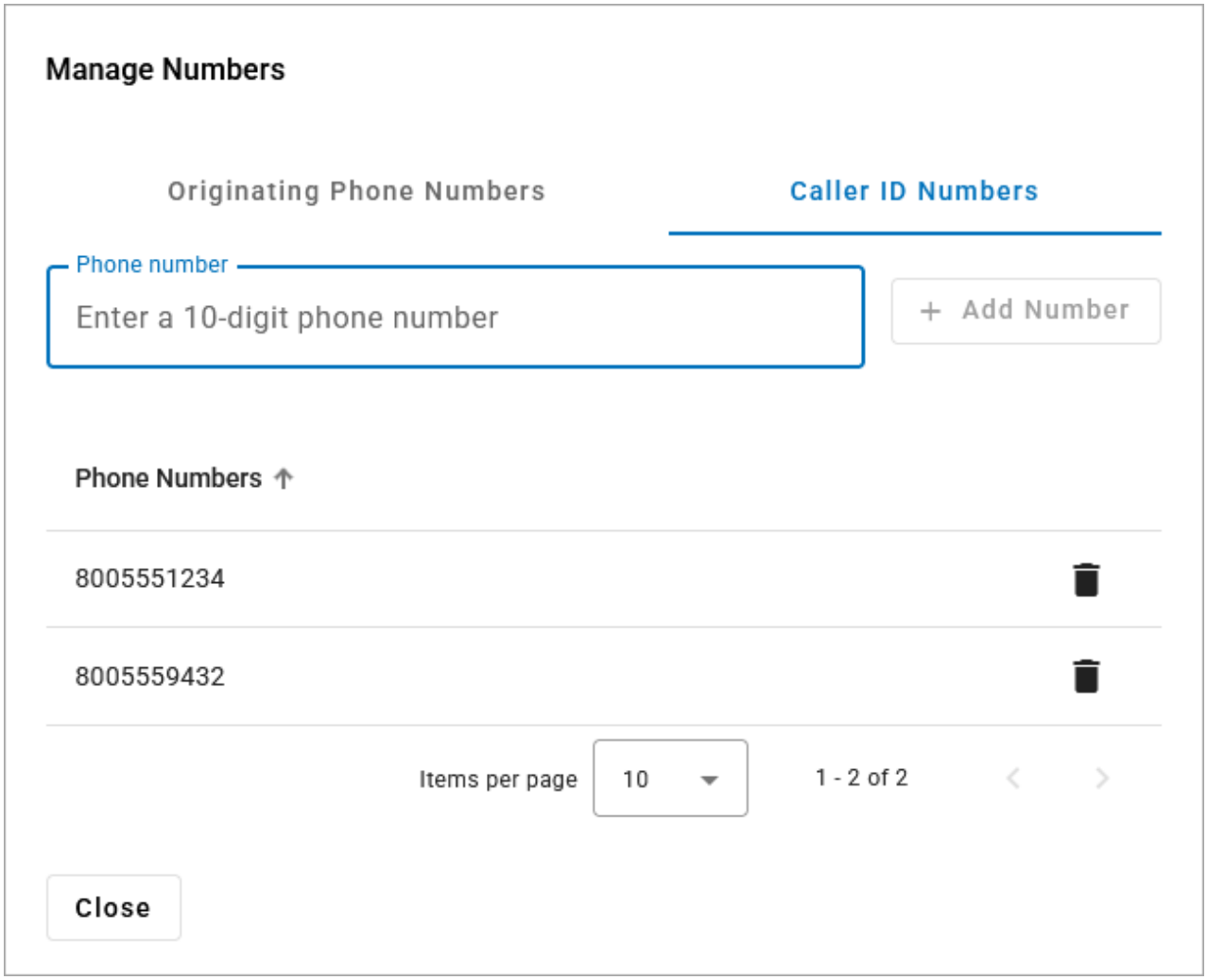
More inclusive patterns take priority. If you assign a custom caller ID to 801* and a different caller ID to 8015551234, the 801* assignment takes precedence. This happens regardless of the order they appear in the system.

© 2026 Cymbus, Inc.

Caller ID Numbers

In the **Manage Numbers** modal, select the **[Caller ID Numbers tab]**, then enter any 10-digit phone numbers that will be used as caller ID. These numbers will be mapped to originating phone numbers later.

To remove a custom caller ID number from the list, select **Delete** on the right. If the number was assigned to an originating number, the assignment will also be deleted.



Map Assignments

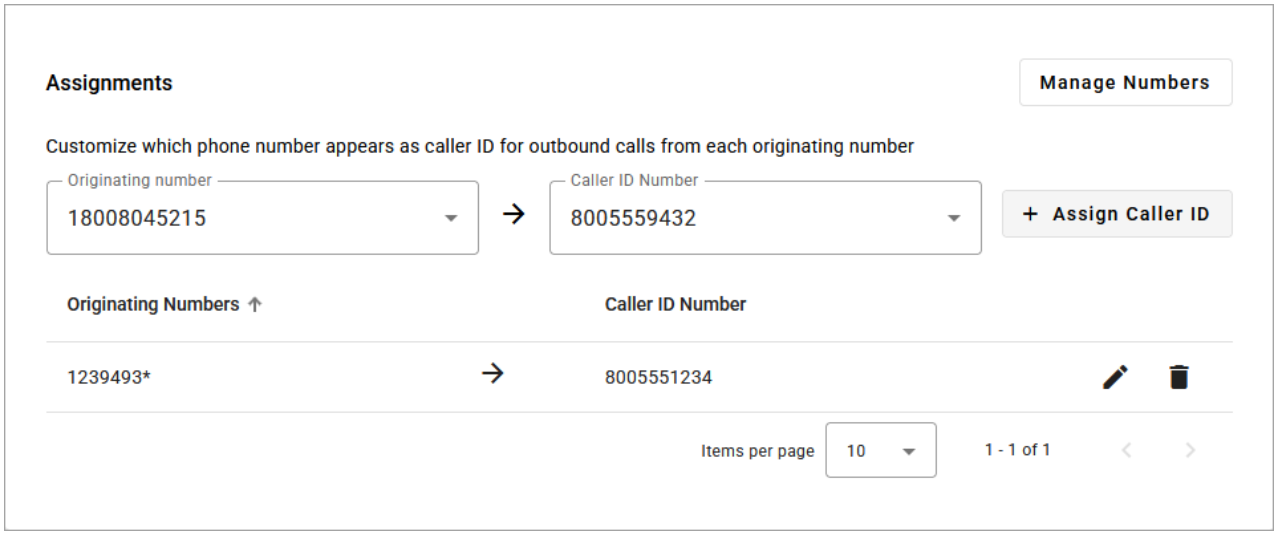
Now that your numbers are defined, map each number so Alianza knows which custom caller ID to use for each originating number. Caller ID assignments take effect immediately for new calls.

1. Go to **SIP Trunk > Custom Caller ID**.
2. Under **Assignments**, select an originating number from the first menu.
3. Select a caller ID number from the second menu.

© 2026 Cymbus, Inc.

4. Select **[Assign Caller ID]** to save the pairing.

Repeat these steps for each originating number you need to map.



One Caller ID Per Originating Number
Each originating number can be assigned to only one caller ID number. A custom caller ID can be assigned to multiple originating numbers, but not the reverse. If you submit a duplicate originating number, it will overwrite the previous assignment.

Edit an Assignment

The caller ID number for each originating number can be modified as needed.

1. Locate the originating number in the list, then select **Edit** on the right.
2. In the *Assign Caller ID* field, select a new caller ID number.
3. Select **[Save]**.

Delete an Assignment

To remove the mapping between an originating number and a caller ID, locate the assignment in the list and select **Delete** on the right.

To delete a phone number entirely (whether originating or custom caller ID), go back to **Manage Numbers** and select **Delete**. Any assignments for that number will also be deleted. Phone numbers assigned to the SIP trunk cannot be deleted.

© 2026 Cymbus, Inc.

Disable Custom Caller ID for SIP Trunking

To disable Custom Caller ID for SIP Trunking for all accounts on your partition, contact your Customer Success Manager for assistance. Once disabled, all existing assignments will remain active but will no longer be accessible in the Admin Portal. If the caller ID assignments are not meant to be permanent, please remove them before requesting to disable the feature.

Trunk Groups

SIP trunk groups are essential for businesses seeking to optimize their voice communication infrastructure. By grouping trunks together, organizations can quickly update the routing settings for all the trunks in just a few clicks, streamlining the administration, configuration, and maintenance of their voice services into one process.

For example, if trunks are grouped by region and one region experiences a large influx of calls, it would take only a few clicks to update the settings for all trunks in the group to fail over to another SIP trunk or even another region (group), eliminating all the time that would have been needed to update each trunk individually.

Shared vs Independent Settings

SIP trunks assigned to a group share call forwarding, overflow routing, and inbound failover routing settings. These group settings take precedence over the configuration set on the individual SIP trunks within the group. However, all other settings continue to be managed at the individual trunk level.

See Manage SIP Trunks for details.

Shared Group Settings	Independent SIP Trunk Settings

• Forwarding settings
• Overflow routing
  • Overflow trunks
  • Forward on overflow settings
• Inbound failover routing
  • Failover trunks
  • Forward on failure settings
	• IP authentication
	• Assigned phone numbers
	• 911 callback number
	• Primary phone number
	• Local Services
	• Dialing digits
	• Concurrent calls allowed
	• Assigned extensions
	• Calling plans

© 2026 Cymbus, Inc.

Add or Manage SIP Trunk Group

Log in to the Voice Portal and go to **Account > SIP Trunks**. From here, select an existing trunk to view or modify the settings, or click **[+ Add SIP Trunk]** in the top right to create one, then fill out or modify the information below.

Note
SIP trunks must already be created on the account before they can be added to a group. See Manage SIP Trunks for details.

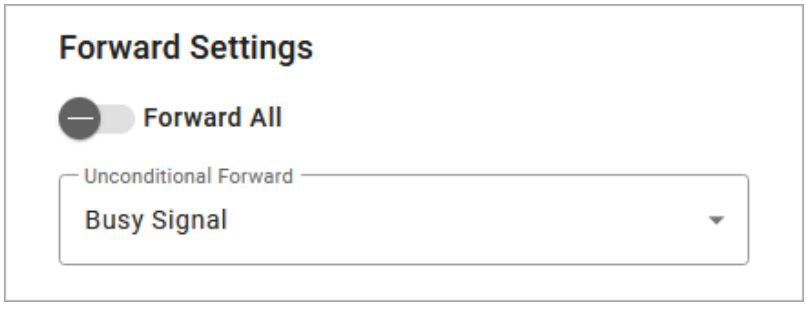
Group Name

Enter a name for the group that is less than 25 characters.

Forward Settings

Check this box to forward *all* inbound calls intended for the SIP trunks in this group to a specific destination. Forwarding destinations include:

- User (select a user)
- Auto-Attendant (select an auto-attendant)
- Voicemail (select a voicemail box)
- Telephone Number (enter an on- or off-net phone number)
- Busy Signal

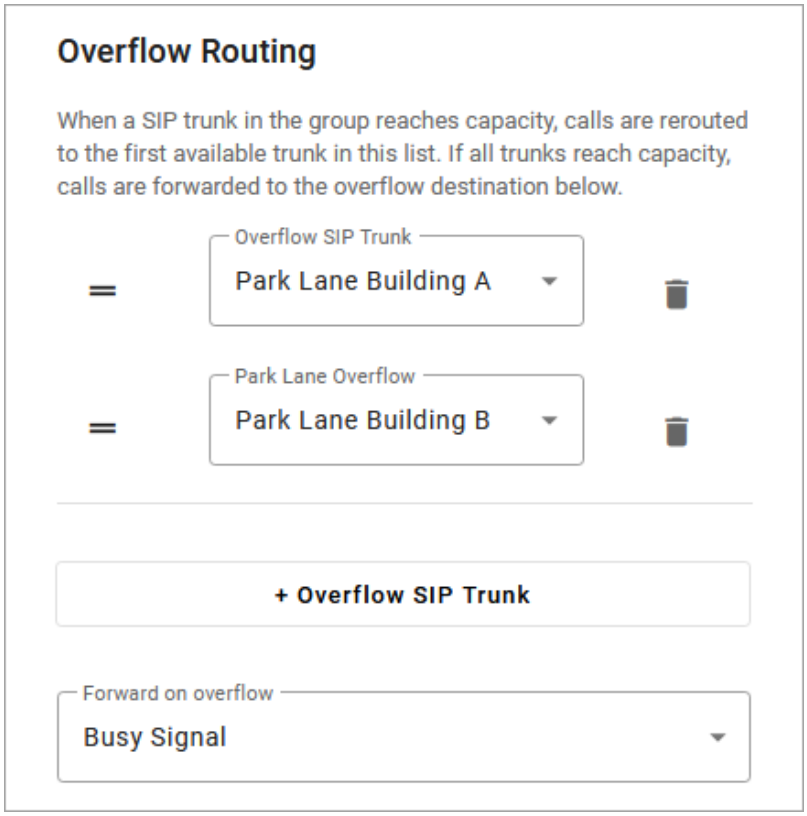


Overflow Routing

When a SIP trunk in the group reaches capacity, meaning it has as many calls as allowed by the concurrent call setting on the individual SIP trunk, calls are rerouted to the first available trunk in this list. If all trunks reach capacity, calls are forwarded to the overflow destination below.

© 2026 Cymbus, Inc.

- **Add Overflow SIP Trunk.** Select a SIP trunk that inbound calls will fail over to once a trunk in this group reaches capacity. Add as many trunks as needed in priority order. To **reorganize** the SIP trunks, click = and drag it to the new location.
- **Forward on overflow.** If all SIP trunks in the group reach the concurrent call limit, calls will be forwarded to the following destination:
  - User (select a user)
  - Auto-Attendant (select an auto-attendant)
  - Voicemail (select a voicemail box)
  - Telephone Number (enter an on- or off-net phone number)
  - Busy Signal



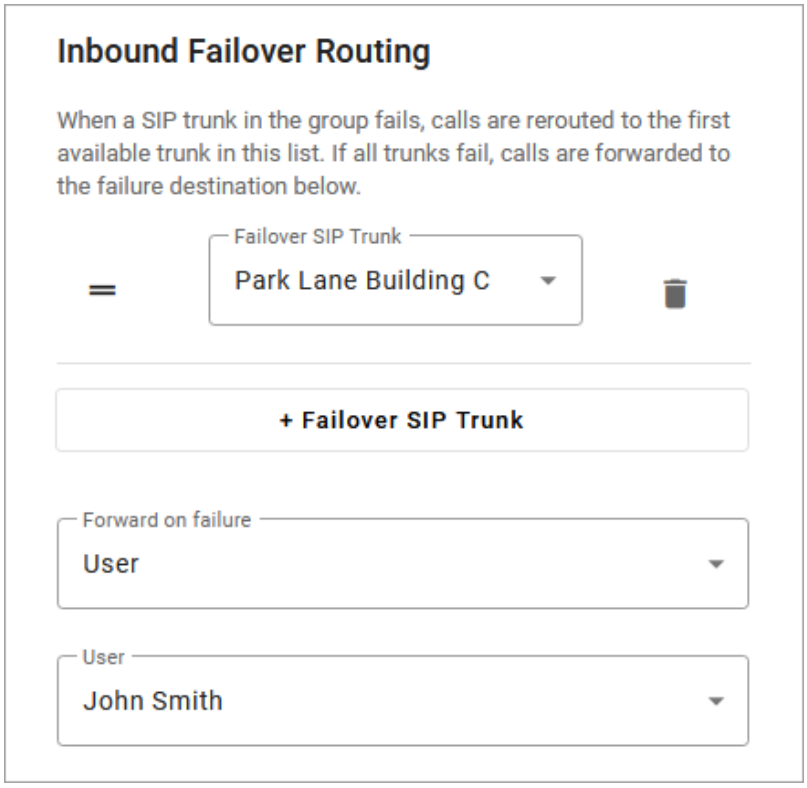
Inbound Failover Routing

When a SIP trunk in the group fails, meaning it cannot register to the platform, calls are rerouted to the first available trunk in this list. If all trunks fail, calls are forwarded to the failure destination below.

Note
Calls being routed to SIP trunks that are not in this group will *not* follow that SIP trunk's fail over routing configuration.

© 2026 Cymbus, Inc.

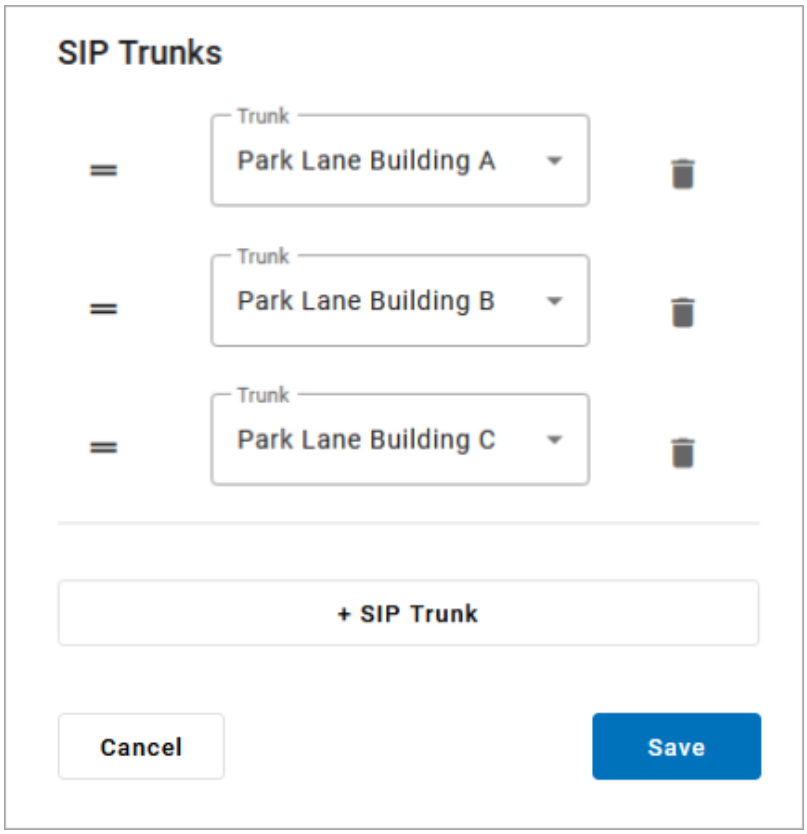
- **Add Failover SIP Trunk.** Select a SIP trunk that inbound calls will fail over to. Add as many trunks as needed in priority order. To **reorganize** the SIP trunks, click = and drag it to the new location.
- **Forward on failure.** Select what happens to inbound calls if all trunks fail:
  - User (select a user)
  - Auto-Attendant (select an auto-attendant)
  - Voicemail (select a voicemail box)
  - Telephone Number (enter an on- or off-net phone number)
  - Busy Signal



SIP Trunks

1. In the **SIP Trunks** section, do one of the following:
   - To **add** a SIP trunk to the group, click **[+ SIP Trunk]** and select a trunk.
   - To **remove** a SIP trunk from the group, click **Trash** on the right.
   - To **reorganize** the SIP trunks, click = and drag it to the new location. Functionally, the order of the trunks doesn't matter, but you can organize them as you'd like.
2. When you're done, click **[Save]**. The changes will be applied immediately.

© 2026 Cymbus, Inc.



© 2026 Cymbus, Inc.

Extension Dialing

For environments with a blend of telephony technologies, SIP trunk extension dialing will reduce phone costs and improve local communications. It allows you to assign extensions to SIP trunks *and* Business Cloud Communications users on the same account, enabling those extensions to dial each other. This means that:

- A user with an extension on the SIP trunk can dial the extension of an IP phone.
- A user with an IP phone can dial an extension on the SIP trunk.

In one example, we helped a retirement community radically overhaul their ease of dialing and reduce costs. The community has an onsite nursing wing, assisted living apartments, and private retirement cottages that needed to bridge the communication gap between their onsite PBX connected by a SIP trunk and IP phones connected to hosted PBX lines. The SIP trunk extension dialing feature enables the residents and caretakers to reach anyone in the community via their 3-4 digit extensions, regardless of their location and telephone technologies.

Assign Extensions to SIP Trunk

Here's how you do it:

1. First, go to **Account > Settings > Devices** and check your settings. For extension dialing to function properly, **Dialing Behavior** must be set to *Open Dialing* or an option that allows an extension.
2. Next, go to **Account > SIP Trunks > Trunks**.
3. Select a SIP trunk or add a new one.
4. Under **Definition**, assign extensions to the SIP trunk. You can enter single extensions, variable extensions, or an extension range in a string; separate each value by a comma.
    - **Single:** 2100 = Extension 2100
    - **Variable:** 21XX = All extensions between 2100 and 2100
    - **Range:** 2110-2199 = All extensions between 2100 and 2199
    - **String:** 4200-5500, 5501, 5578, 68XX

Extensions Must Be Unique

A single extension cannot be assigned to multiple locations (user, group, or SIP trunk). If an end user is assigned an extension that overlaps with an extension range assigned to a SIP trunk, calls to that extension will be routed to the *end user*, not to the SIP trunk.

Additionally, if an end user extension overlaps an extension range assigned to a SIP trunk, calls to that extension will be routed to the user and **not** the SIP trunk.

© 2026 Cymbus, Inc.

Local Services

SIP Trunk Local Services enables the SIP trunk to translate local service calls (like 211, 411, etc.) from a 3-digit number to a 10-digit number, so it doesn't have to be configured on the PBX.

Local Services is enabled on a per-trunk basis. Once enabled, the voice server will accept and route 3-digit N11 codes (411, 611, etc.) and 7-digit local dialing numbers from the SIP trunk. SIP trunks will no longer need to translate these numbers into 10-digits before they're sent to the voice server.

- **Emergency Numbers.** Whether or not Local Services is enabled, calls to 911, 933, and 988 will route correctly. Geographic data used for public service functions and 7-digit dialing will be assigned to the SIP trunk based on its primary phone number.
- **International Numbers.** After enabling Local Dialing, users will need to dial 011 before international numbers, even if the SIP trunk was previously configured to allow international dialing without it.
- **N11 Numbers.** In some cases, Local Services must be enabled for SIP trunk users to dial N11 codes. Refer to Social & Public Services for more detailed information.

Supported Dialing Patterns

Pattern	Description
International Long Distance	011+
National Long Distance	1+
Local Dialing	7- and 10-digit numbers, translated to 1+NPA+dialed number
7-digit Local Dialing	Translated to 1+NPA+dialed number
10-digit Local Dialing	Translated to 1+dialed number

Note

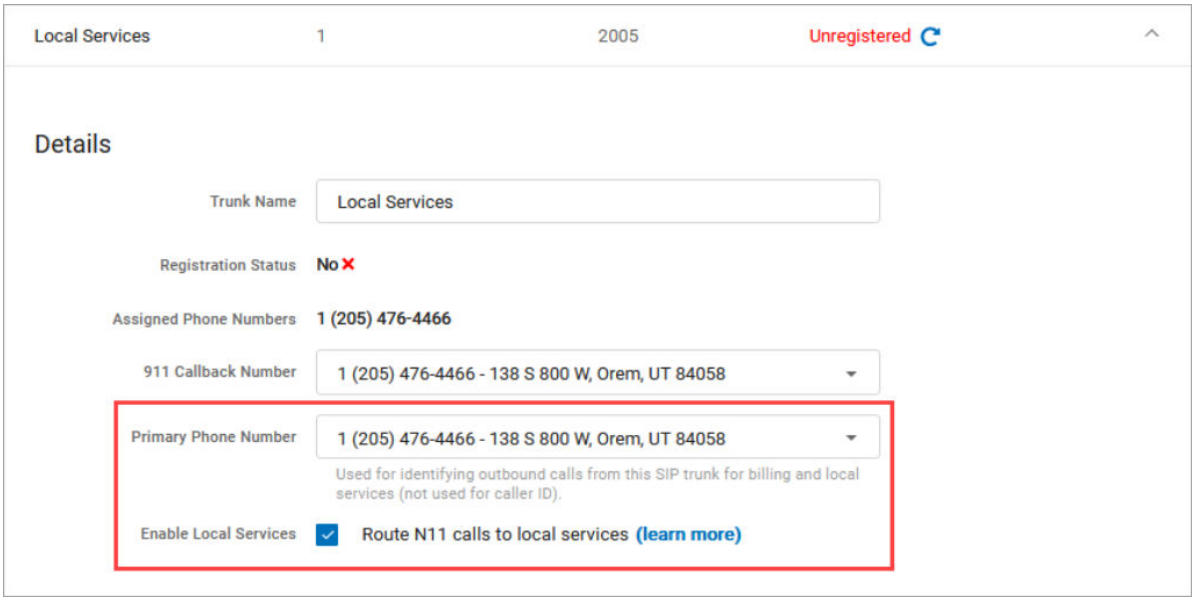
After enabling Local Dialing, users must dial *011* before international numbers, even if the SIP trunk was previously configured to allow international dialing without it.

Enable Local Services

Getting started is a two-part process: Enabling Local Services in the Alianza Admin Portal and ensuring the end user's SIP trunk/PBX is configured to use it.

© 2026 Cymbus, Inc.

1. In the Admin Portal, search for the account and then go to **Account >Trunks**.
2. Locate an existing trunk and click **Edit**, or click **[+ Add SIP Trunk]** and fill out the information to set up a new one.
3. Under **Details**, check **Enable Local Services** and select a primary phone number.



A primary phone number is not required, but it is recommended. Alianza determines where to route local service calls based on the address associated with this number.

If you're setting up a SIP trunk for the first time and a primary phone number is not available, select *None* and update this field when a phone number becomes available. In the meantime, be sure to provide geographic information to the SIP trunk configuration; otherwise, local services dialing will fail, including Directory Assistance, Call Public Services, and 7-digit dialing.

4. Save the SIP trunk configuration.
5. Next, update the end customer's SIP trunking device to allow the new configuration. This process will vary for each device.

© 2026 Cymbus, Inc.

Social & Public Services

The following N11 codes provide quick three-digit dialing access to special services in the United States and Canada, based on the caller's address, without the need for an area code.

Code	Description
211	**Essential Community Services** Access to community information and referral services, such as essential needs, crisis, and disaster assistance. Visit http://www.211.org/ to learn about services in your area.
411	**Directory Assistance** Phone service used to look up a published telephone number and/or address listing.
511	**Traveler Information (US)** Local hotline for real-time information regarding traffic and road conditions. Not available in all states.
611	**Customer Service** Dials Customer Service.
711	**Telecommunications Relay Service** TRS uses operators to facilitate phone calls between people with hearing and speech disabilities and other individuals. A TRS call may be initiated by a person with or without a disability. Visit http://www.fcc.gov/ to learn more.
811	**Utility Location Services (US)** “Call Before You Dig” routes the caller to their local utility location services. Call a few days before beginning an excavation project to find out the location of underground utilities and reduce the risk of serious damage.
811	**Canadian Health Services (CAN)** Call to speak to a local health care professional about medical advice, mental health, healthy eating, and more.
911	**Emergency Services** Calls to 911 (US or CAN) are sent to the nearest Public Safety Answering Point (PSAP) based on the registered address. The callback number and address are available to the PSAP on each call.
933	**Emergency Services Validation** Calls to 933 are sent to the caller’s emergency services provider, who will then connect the call to their automated 911 verification service. The service will play back the dialing phone number and the address associated with it.

© 2026 Cymbus, Inc.

Code	Description
988	**Suicide Prevention Hotline** Contact the National Suicide Prevention Lifeline (US) or Talk Suicide Hotline (CA) to speak with a trained crisis counselor who will listen, offer support, and get them the help they need.

Canadian Support

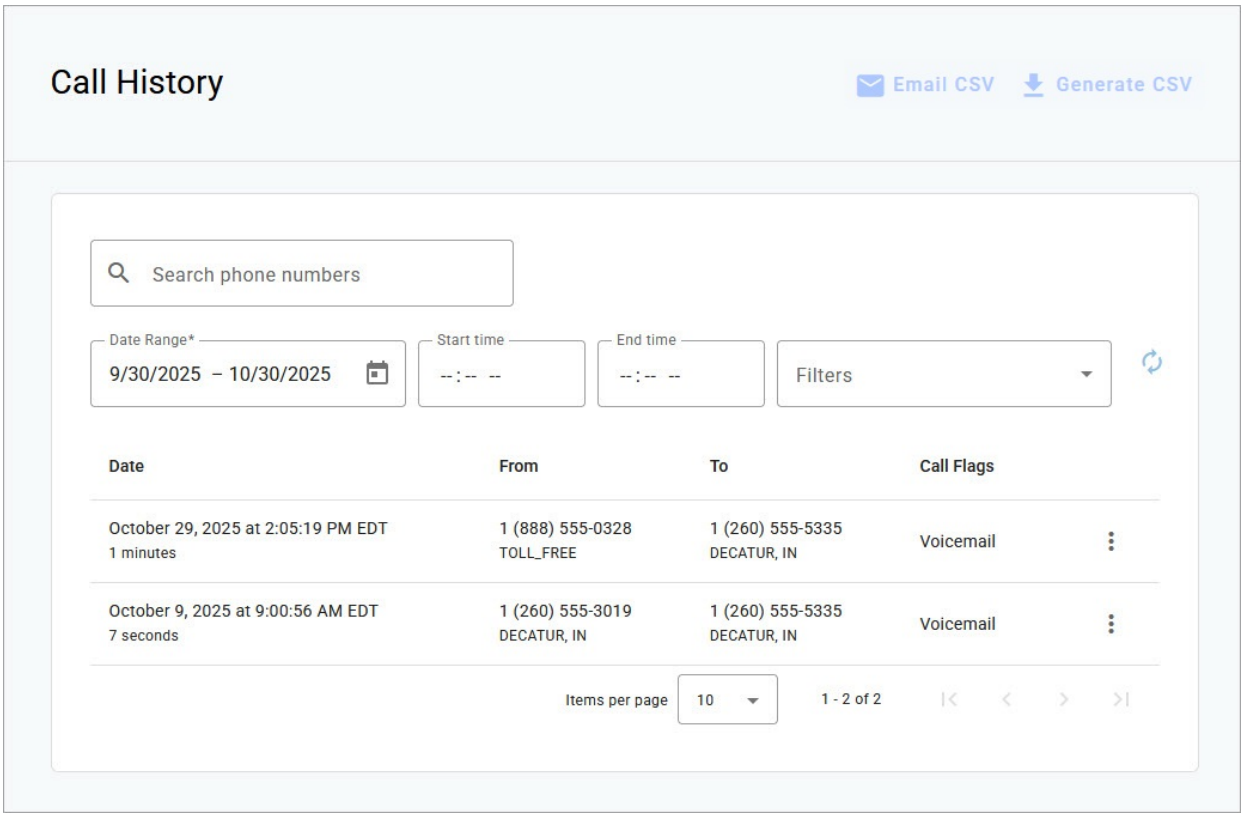
Not all Canadian rate centers support all N11 service codes. If you are unable to call a particular service, it may not be available in your area.

© 2026 Cymbus, Inc.

Call History

Call History holds the records of all calls made and received on the account. Calls are listed in chronological order with the most recent call at the top. Call data is organized into columns that show the date and time of the call, where the call originated (From), where the call terminated (To), the call flag for inbound calls, and the account code used.

At the top right of the page, the current record list can be emailed as a .csv file, or downloaded directly from the portal. See Call History Report Fields for details on what is included in the report.



CDR Storage

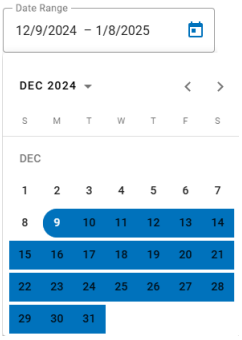
The FCC requires that all carriers keep call detail records for a period of 18 months. While some states defer to the FCC, other states have retention rates that exceed the federal requirement. To be safe, the portal displays call records for the past 18 months, but our database stores call records for a minimum of 3 years.

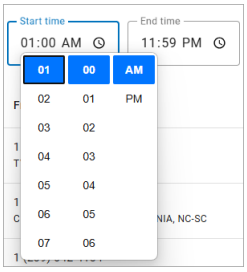
© 2026 Cymbus, Inc.

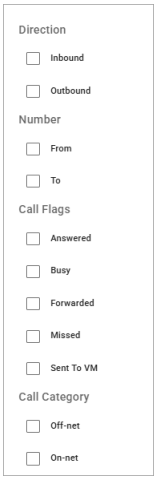
Apply Call Filters

Apply call filters to locate specific call records. Once your parameters are set, the matching call records are displayed below.

- **Search phone numbers:** Search for a specific phone number or extension. Results automatically populate after the first three digits are entered.
- **Date Range:** Modify the date and time ranges or delete them entirely to gather the data you need. By default, the last 30 days of call records are displayed.
- **Start/End Time:** Enter a time range between 12:00 AM and 11:59 PM based on the account's time zone settings.
- **Filters:** Filter the call records by Direction, Number, Call Flags, and/or Call Category. These filters allow you to identify patterns in the calls, such as how many calls are being sent to voicemail, what calls are being missed, etc.
- **Reset:** When you're finished with your search, click **Reset Filters** to remove any parameters and display all calls.







Select Call Options

To view the details for a call, click the ⋮ menu on the right. The option to block the number is also available for inbound calls.

© 2026 Cymbus, Inc.

Block Number

If necessary, you can block an inbound caller from making additional calls to the account.

1. Click **[Block Number]**.
2. Select whether the number should be blocked on the user or the account.
3. Click **[Confirm]** to add the inbound phone number to the blocked caller list.

Details

Call details include the date, time, and length of the call, as well as the cost, origination, and termination information.

Field	Description
Time and Length	When the call started, connected, and ended, what duration of the call was billed, and the actual length of the call.
Cost	The cost of the call, if the call was within the calling plan, and the rate per minute from the plan.
Origination	The number and location of the originating call, if the call came from on or off the network, and any tag that's been assigned to the phone number.
Termination	The number and location of the user who received the call, if they were on or off the network, any tag that's been assigned to the phone number, and how the call was flagged.

Export a Call History Report

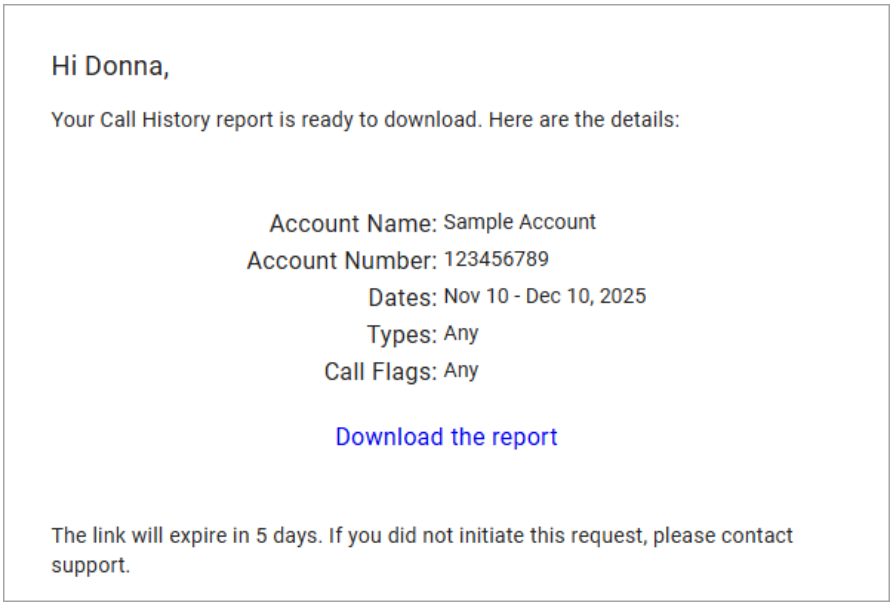
Once you've applied the appropriate filters to locate the data you need, you can export the data into a .csv file for offline use. A report can be emailed to the address on your account, or downloaded directly from the portal.

© 2026 Cymbus, Inc.

Email a Call History Report

1. At the top right of the page, click Email CSV. A banner displays on the page to indicate that your report is being generated.
2. When the file is ready, an email with a link to download the report is sent to the email address in your settings. The link **expires in 5 days** and can only be used once.

   Here's an example of what it looks like:



Hi Donna,

Your Call History report is ready to download. Here are the details:

Account Name: Sample Account
Account Number: 123456789
Dates: Nov 10 - Dec 10, 2025
Types: Any
Call Flags: Any

Download the report

The link will expire in 5 days. If you did not initiate this request, please contact support.

> **Email Address**
> The link to download the Call History report is sent to the email address on your user account. If your email address is not linked to your account yet, contact an account administrator for assistance.

Download a Call History Report

1. At the top right of the page, click Generate CSV. A banner displays on the page to indicate that your report is being generated.
2. When the file is ready, the browser starts downloading it on your device.

Call History Report Fields

This list includes all the fields available in the Call History report which can be emailed (exported) from the portal as a .csv file. Each line in the file represents a call. Your report may not include all available fields.

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
A	AccountBillableAbbrRCName	string	Abbreviated name of the rate center of the account billable phone number.
B	AccountBillableCityName	string	Name of the city of the address associated with the phone number.
C	AccountBillableLocation	string	MSA (metropolitan statistical area) of the address associated with the number.
D	AccountBillableNumber	string	Phone number on the account.
E	AccountBillableState	string	State of the address associated with the rate center.
F	AccountCode	string	Account code tagged on this call.
G	AccountNumber	string	Client-assigned account number of the account to which the call is billed.
H	AcctId	string	Unique ID of account to which the call is billed.
I	ActualCallLengthSeconds	numeric	Length, in seconds, of the call from connect to end.
J	BillCallLengthSeconds	bigint	Length, in seconds, of the call from connect to end rounded according to applied calling plan product.
K	BillingCode	string	Unique code to identify the partition responsible for billing.
L	CallFlagType	string	Indicates if the call was answered on a device, and if not answered on a device, how did it terminate. • Answered • Busy • Forwarded • Missed • Voicemail
M	CallPickupFromId	string	Indicates the object that picked up the call.

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
N	CallPickupById	string	Indicates the object from which the call was picked.
O	CallType	string	Inbound or outbound.
P	CallingPlanProductId	string	Unique ID of the calling plan product with which the call was rated.
Q	CallingPlanProductName	string	Name of the calling plan with which the call was rated.
R	ConnectTime	date/time	Date and time the call was connected. Billing starts at this time.
S	Cost	double	Rated value of call, according to calling plan product.
T	DialedNumber	string	Digits originally dialed to start the call.
U	DisconnectType	string	Indication of which party disconnected the call; "HangUp" indicates the origin, "HangUpOther" indicates termination.
V	EndTime	date/time	Date and time the call ended.
W	ForwardingNumber	string	Phone number the call was forwarded to.
X	ForwardingNumberAbbrRCName	string	Abbreviated name of the rate center of the phone number the call was forwarded to.
Y	ForwardingNumberCityName	string	Associated rate center city name of the phone number the call was forwarded to.
Z	ForwardingNumberLocation	string	MSA (metropolitan statistical area) of the rate center of the number.
AA	ForwardingNumberState	string	State of the associated rate center of the phone number the call was forwarded to.
AB	Id	string	Unique string of characters assigned to each call within the Alianza system.
AC	IdentityAttestLevel	string	STIR/SHAKEN field. A = fully attested or trusted source, B = partially attested, or C = not attested (potential spam).

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
AD	IdentityOriginationId	string	STIR/SHAKEN field. A unique identifier used to identify the source of the call.
AE	IdentitySignOrganization	string	STIR/SHAKEN field. The code for the carrier that performed the signing.
AF	IdentitySignSPCode	string	STIR/SHAKEN field. The code assigned to the service provider that signed the call.
AG	InPlan	boolean	True/False indicator of whether the call was considered "in plan."
AH	LegType	string	Indication of direction of call: • Origination • Termination • Forward
AI	MeanOpinionScoreAverage	numeric	Average MOS for the call.
AJ	MeanOpinionScores	list<string>	List of MOS scores associated with each SIP call leg.
AK	MediaServerType	string	Indication of what media service was used by call, if any.
AL	MetroServiceArea		*Reserved for future use*
AM	OrigAbbrRCName	string	Abbreviated name of the rate center of the phone number that made the call.
AN	OrigCallCategory	string	Type of call that was made.
AO	OrigCarrier	string	Name of the carrier, if applicable.
AP	OrigCityName	string	City for the associated rate center for the phone number that made the call.
AQ	OrigLocation	string	MSA (metropolitan statistical area) of the rate center for the phone number that made the call.
AR	OrigNumber	numeric	Phone number that made the call.

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
AS	OrigState	string	State of the associated rate center for the phone number that made the call.
AT	PartitionId	string	Unique ID of client partition to which the associated account belongs.
AU	RateLocalFromNumber		*Reserved for future use*
AV	RatePerMinute	double	Per-minute rate for call, according to the calling plan assigned to the user making the call.
AW	RateType		Indication of why the call was rated the way that it was. • Local • OnPlanMinutes • OnPlanRated • OffPlanRated • Free • TollFree • 411 • Operator Local requires the calling plan to be set up with Unlimited Local, and the calls are rated at $0.
AX	ReferenceId	string	Unique ID of the acting or responsible party on the associated account to which the call was billed.
AY	ReferenceName	string	Name of acting or responsible party.
AZ	ReferenceType	string	Type of object to which the call is billed. • SIP_TRUNK • END_USER • ACCOUNT • BUSINESS_LINE

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
BA	SessionId	string	Internal softswitch session ID.
BB	SipCallIds	set<string>	List of SIP callIds associated with the call.
BC	StartTime	date/time	Date and time the call started ringing.
BD	TermAbbrRCName	string	Abbreviated name of the rate center of the phone number that received the call.
BE	TermCallCategory	string	Type of call that was made.
BF	TermCarrier	string	Name of the carrier, if applicable.
BG	TermCityName	string	Associated rate center city name of the phone number that received the call.
BH	TermLocation	string	MSA (metropolitan statistical area) of the rate center of the phone number that received the call.
BI	TermNumber	string	Phone number that received the call.
BJ	TermState	string	State of the associated rate center of the phone number that received the call.
BK	OrigCnam	string	Originating caller's name.
BL	TermCnam	string	Terminating caller's name.
BM	ForwardingCnam	string	Forwarding caller's name.
BN	RemoteChargeInfo	string	The external charge number assigned to calls from this SIP trunk.
BO	CustomCallerID	string	The custom caller ID sent with this call.
BP	VerStat	string	STIR/SHAKEN field. String from the *verificationResponse* containing: • **TN-Validation-Passed.** The number passed the validation. • **TN-Validation-Failed**. The number failed the validation. • **No-TN-Validation.** No number validation was performed.

© 2026 Cymbus, Inc.

#	Field Name	Type	Description
BQ	VerStatReason	string	STIR/SHAKEN field. String of text from the *verificationResponse* message used in case of failed verification. • BAD_IDENTITY_INFO • CLAIM_TO_SIP_MISMATCH • INVALID_IDENTITY_HEADER • MALFORMED_IDENTITY_HEADER • STALE_DATE • UNSUPPORTED_CREDENTIAL • UNSUPPORTED_PASSPORT_FORMAT
BR	CorrelationData		
BS	ApplicationData		
BT	OrigNumberTags	string	Tag(s) assigned to the number on an outbound call.
BU	TermNumberTags	string	Tag(s) assigned to the number on an inbound call.

© 2026 Cymbus, Inc.

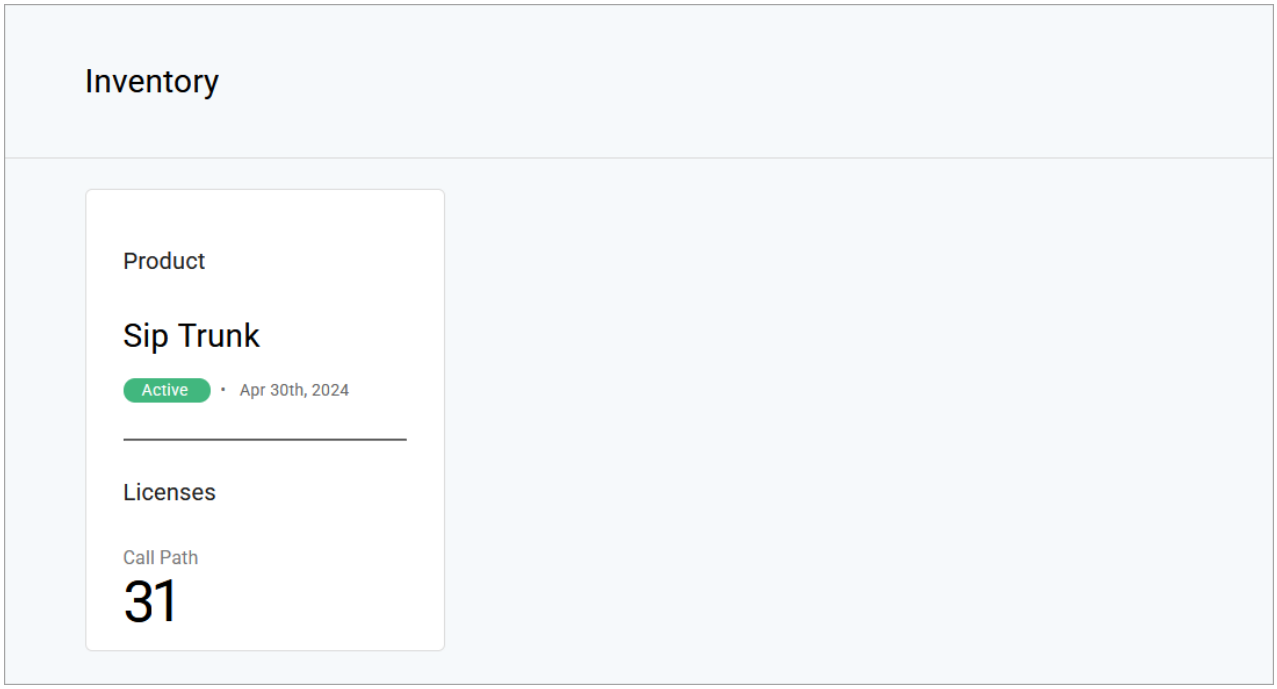
Analytics

The Analytics section presents metrics about the account.

Inventory

The inventory dashboard, viewable only to Account Managers and Super Admin users, displays a read-only view of the products, licenses, and add-ons in an account.

Each product is organized by name, the account status (Active, Suspended, or Disabled), the date the status was last updated, and the licenses that are included.



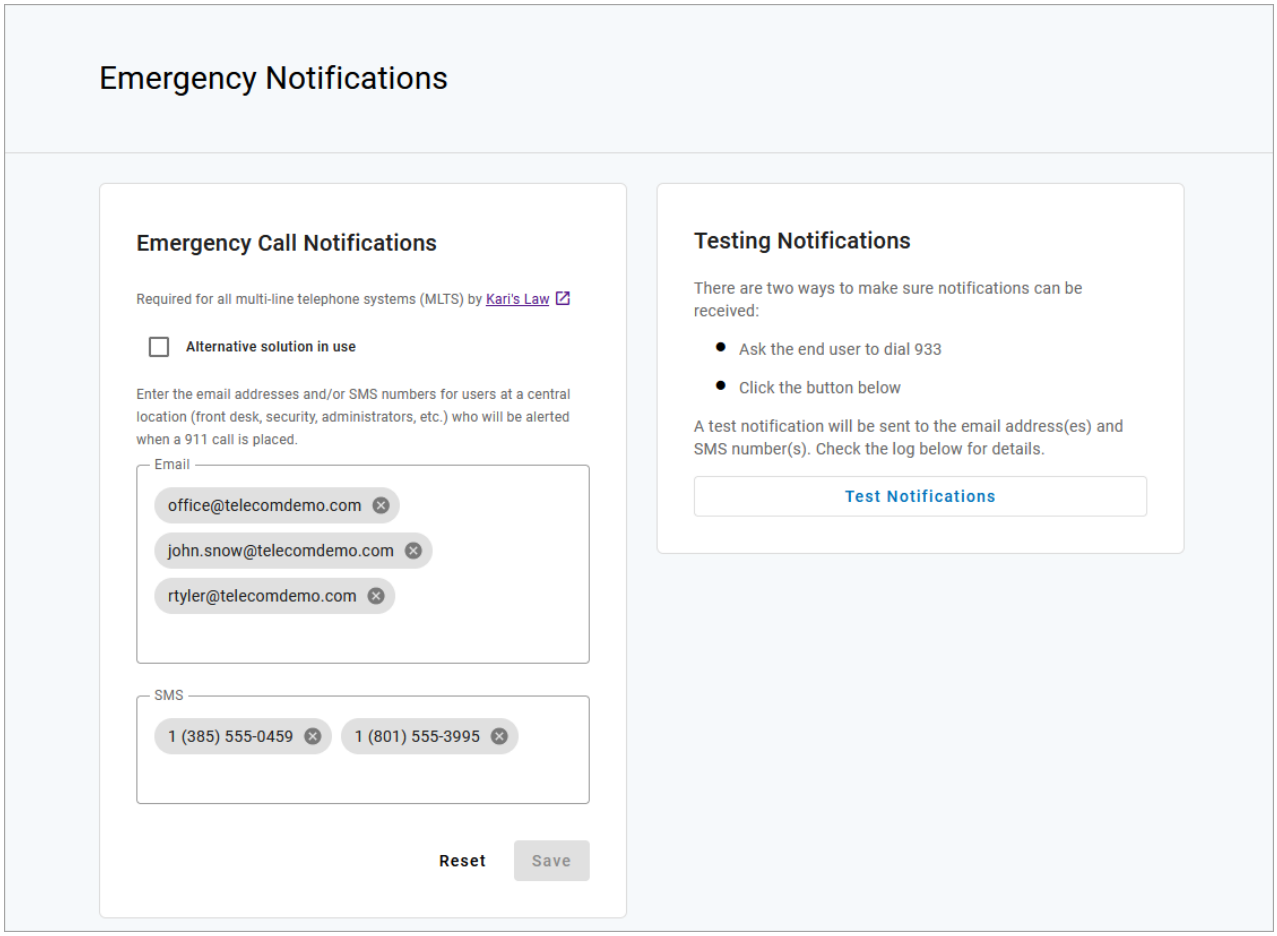
© 2026 Cymbus, Inc.

Account Settings

Emergency Notifications

In recent years, the FCC has passed Kari's Law and RAY BAUM's Act to help expedite response to emergency services to callers and improve outcomes. As part of Kari's Law, all multi-line telephone systems (MLTS) must be preconfigured to send a notification to an on-site location (like a front desk or security office) when a 911 call is made.

For Emergency Notifications to work, each phone number on the account must be successfully configured with a valid E911 record, which includes the physical address where the device is located and any other information necessary to precisely identify the caller's location. It is the end user's responsibility to keep this information up to date.



© 2026 Cymbus, Inc.

Alternative Solution

Emergency Notifications are *required* for any and all MLTS manufactured, imported, sold, leased, or installed after **February 16, 2020**. If your account already meets this requirement with an on-premises solution, select *Alternative solution in use*.

Configure Emergency Notifications

It is important that you choose to notify a central location where someone will see or hear the notification, such as a managed distribution list of on-site personnel (front desk, security office, administrators, etc.), rather than an individual who may or may not be at the location 100% of the time. While there isn't a limit on how many contacts can be entered here, make sure the number is reasonable for your organization.

1. In the portal, go to **Settings > Emergency Notifications**.
2. Identify the email address(es) and SMS-capable phone number(s) that will be notified when an emergency call is placed from a number on the account. Enter those email addresses and phone numbers in the portal and click **[Save]**.

Now, when someone on your account dials 9-1-1, the emergency call is processed and a notification is sent to the recipients configured in the portal, so they are made aware of the situation and can assist emergency responders upon arrival.

Test Notifications

We strongly recommend testing the service after setting or changing the configuration to ensure it is properly configured. There are two ways to do this:

- Click [**Test Notifications]** to send notifications to the email address(es) and SMS number(s) configured for the account.
- Ask the end user to dial 933 to verify their emergency call record with their E911 provider.

  The call will be connected to an automated 911 verification service, which will play back the dialing phone number and its associated address. The end user is expected to contact their service provider if the information is incorrect or any changes are needed.

The end user should confirm that all recipients have received the notifications and that they understand its purpose.

Example Texts

SMS notifications include the type of message and caller details.

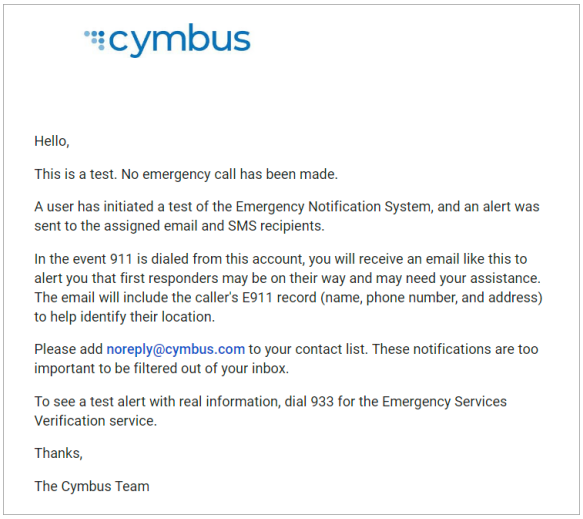
```
911 NOTIFICATION: Shirley Bennent (801-489-7891) 20MAY20 6:15 PM MST
Location: 1242 N 400 W, Suite 980, Pleasant Grove UT 84023

933 NOTIFICATION: Shirley Bennent (801-489-7891) 20MAY20 6:15 PM MST
Location: 1242 N 400 W, Suite 980, Pleasant Grove UT 84023
```

© 2026 Cymbus, Inc.

```
TEST NOTIFICATION: In the event a 911 call is placed, you will receive
a text like this one to notify you that first responders may be on their
way and may need your assistance.
```

Example Emails

The test notification will let you know this is only a test. In the event 911 is dialed, the notification email will include the name, phone number, and address on the E911 record, and additional details including the name of the device owner, the extension, device type, line name, and MAC address.



cymbus

Hello,

This is a test. No emergency call has been made.

A user has initiated a test of the Emergency Notification System, and an alert was sent to the assigned email and SMS recipients.

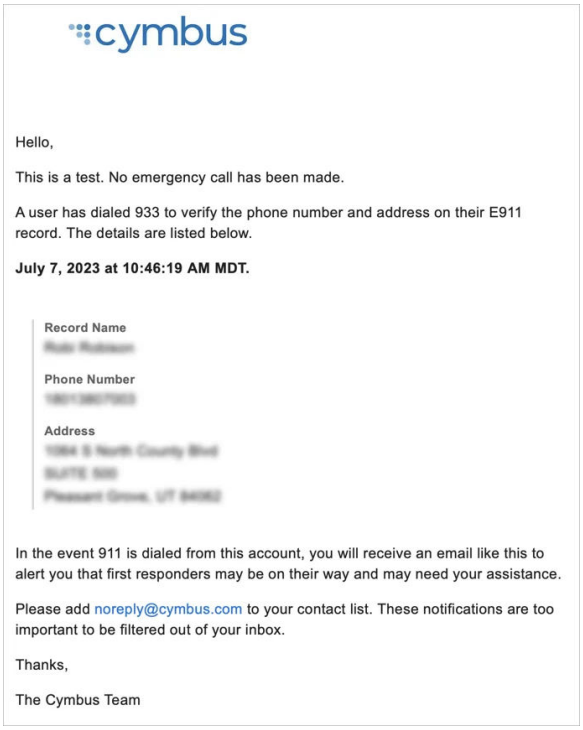
In the event 911 is dialed from this account, you will receive an email like this to alert you that first responders may be on their way and may need your assistance. The email will include the caller's E911 record (name, phone number, and address) to help identify their location.

Please add noreply@cymbus.com to your contact list. These notifications are too important to be filtered out of your inbox.

To see a test alert with real information, dial 933 for the Emergency Services Verification service.

Thanks,

The Cymbus Team



cymbus

Hello,

This is a test. No emergency call has been made.

A user has dialed 933 to verify the phone number and address on their E911 record. The details are listed below.

July 7, 2023 at 10:46:19 AM MDT.

Record Name
[redacted]

Phone Number
[redacted]

Address
[redacted]

In the event 911 is dialed from this account, you will receive an email like this to alert you that first responders may be on their way and may need your assistance.

Please add noreply@cymbus.com to your contact list. These notifications are too important to be filtered out of your inbox.

Thanks,

The Cymbus Team

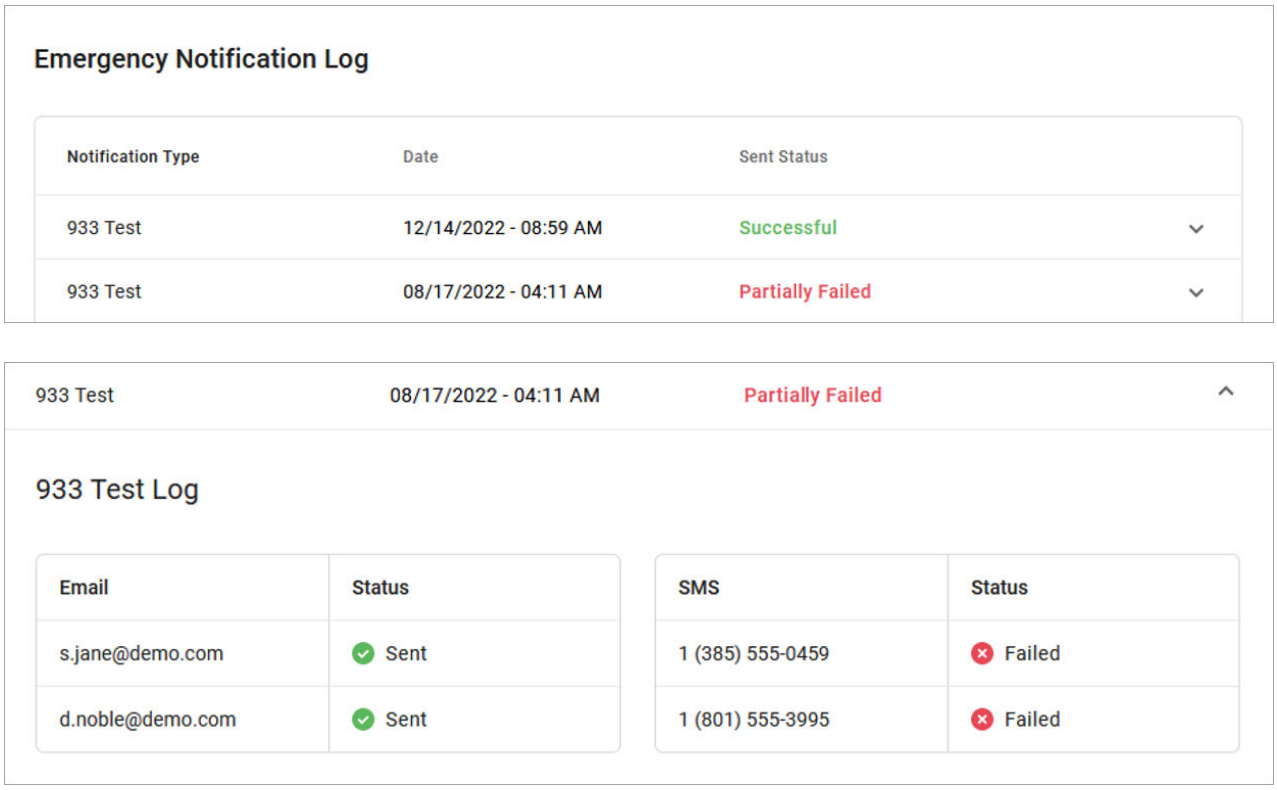
Emergency Notification Log

The Emergency Notification Log contains a complete history of all test and emergency call notifications sent for this account. The notification type is identified on the left, followed by the date and time and sent status:

- **Successful:** The notification was successfully sent to all parties.
- **Partially Failed:** The notification was sent to some but not all parties.
- **Failed.** The notification was not sent.

Expand an entry for details:

© 2026 Cymbus, Inc.

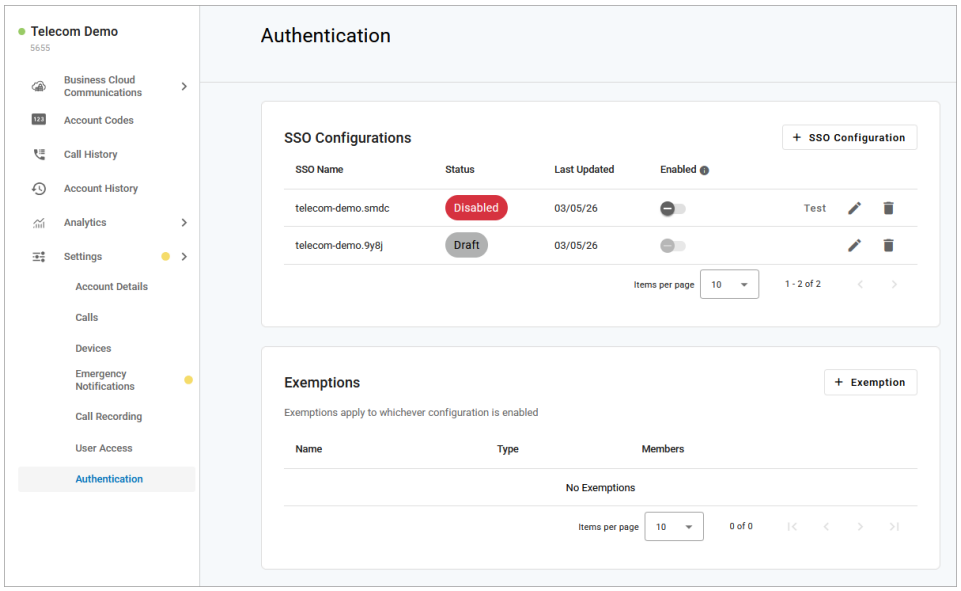


SSO Authentication

Single Sign-On (SSO) is an authentication method that allows users to access multiple applications using a single set of credentials. Once a user has signed in through their organization's Identity Provider (IdP), they can move seamlessly between connected systems without being prompted to log in again. This reduces friction and password fatigue for end users, while giving administrators the ability to enforce consistent security policies, such as multi-factor authentication (MFA), across all connected applications from a single place.

If you would like your employees to access the voice portal using the same single sign-on process they use for accessing other tools, you can set that up here, in the Authentication section of the account.

© 2026 Cymbus, Inc.

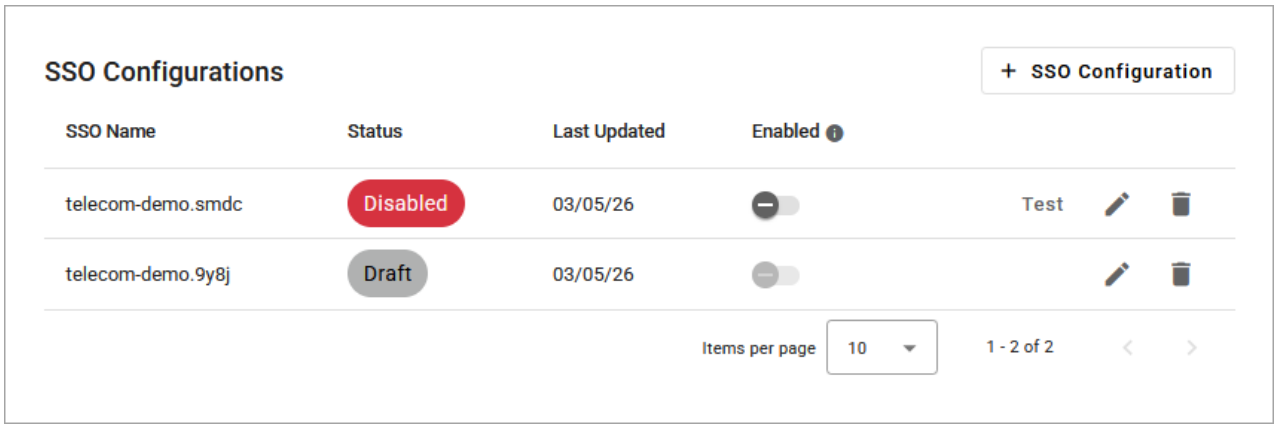


SSO Configurations

The SSO configurations section displays every SSO configuration set up on the partition. From here, you can create and manage your configurations, saving as many drafts as needed.

Keep in mind that only one SSO configuration can be enabled at a time. To switch to a different configuration, disable the current one and then enable the desired one.

See also: Manage Single Sign-On



Field	Description
SSO Name	System-generated name for the configuration. This cannot be changed.

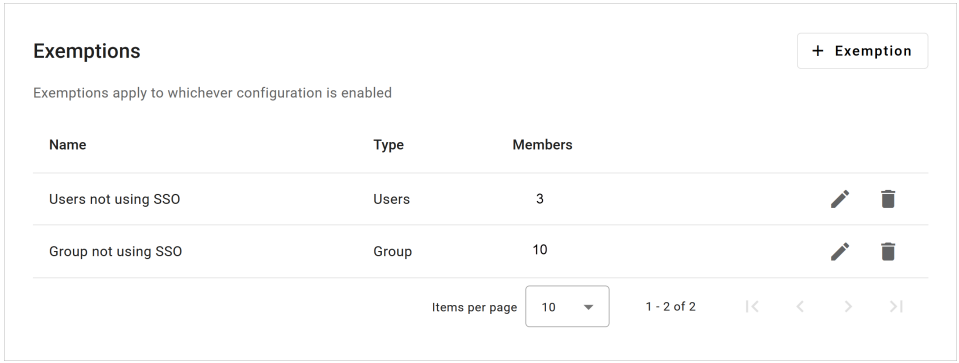
© 2026 Cymbus, Inc.

Field	Description
Status	Will display the status of the SSO configuration, these include: • **Enabled.** The configuration is being enforced on the account. • **Disabled.** The active SSO configuration has been made inactive. • **Draft.** The SSO Account Name was generated and setup has begun, but has not been completed. • **Ready.** The configuration is complete and ready to test before being enabled.
Last Updated	Date the configuration was last created, edited, enabled, or disabled.
Enabled	Toggle on or off to manage which completed SSO is used by the account. • When enabling or changing which SSO configuration is being used, be sure customers are informed of the change.
Test	Test the connection between the IdP and the SSO configuration.
Edit	Modify your IdP information and the sign-in public key.
Delete	Remove the configuration from the account. • Configurations can only be deleted when they are **not** enabled.

Exemptions

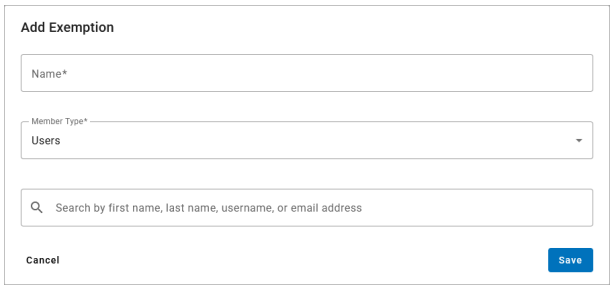
Use this section to exempt specific users or groups from using the enabled SSO on the account. Excluded users will fall back to Alianza's default login process, or can be configured with the partition's SSO instead. Contact Customer Service for details.

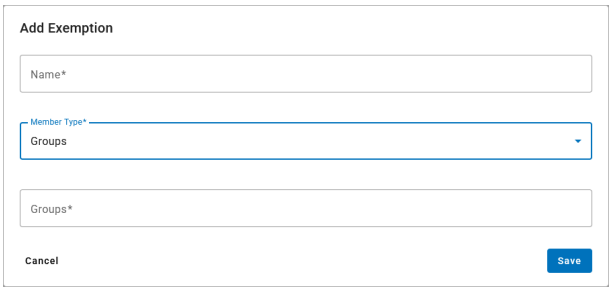
© 2026 Cymbus, Inc.



Add Exemptions

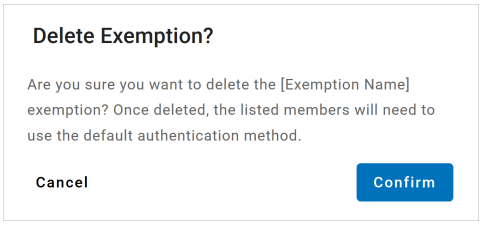
1. Go to **Account > Settings > Authentication**.
2. In the **Exemptions** section, click **[+ Exemption]**.
3. Enter a name to reference this list of exemptions.
4. Select if the exemption will apply to specific user(s) or group(s) of users.
5. Search for the user(s) or group(s) to be exempt from using the SSO configuration.
6. When complete, click **[Save]**.





Remove Exemptions

1. Go to **Account > Settings > Authentication**.
2. In the **Exemptions** section, click the **trash** icon next to the user or group list to be removed.
3. Click **[Confirm]** in the pop-up window to complete the deletion.



© 2026 Cymbus, Inc.

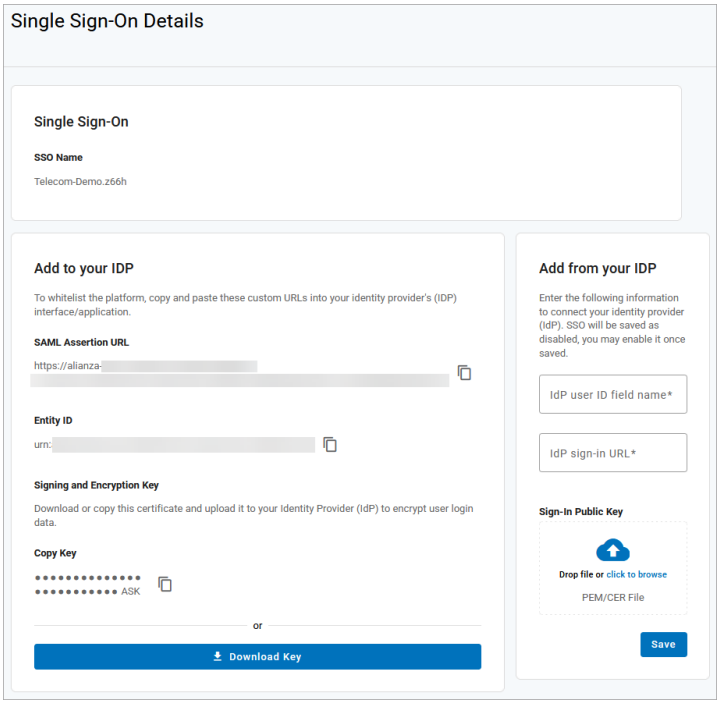
Manage Single Sign-On

Allowing specific login experiences for each customer account is possible with Account-level SSO. These SSO settings can be managed in **Account > Settings > Authentication** by end user Account Managers .

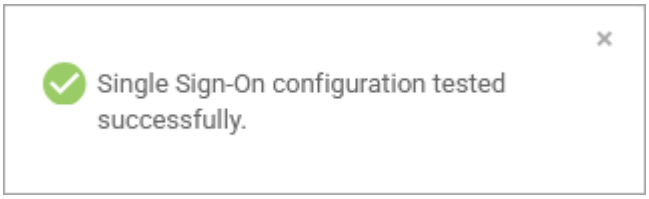
Add SSO Configuration

1. Go to **Account > Settings > Authentication**.
2. Click **[+ SSO Configuration]**.
3. The SSO name and custom URLs are automatically created.
4. In the **Add to your IDP** section, copy the following information and add it to your identity provider's (IdP) interface/application:
    - SAML
    - Entity ID
    - Signing and Encryption Key
5. In the **Add from your IDP** section, enter the following information from your IdP:
    - **IdP user ID field name.** The name of the attribute in your IdP's SAML assertion that uniquely identifies each user on your side. Common values include `email`, `username`, or `uid`. Alianza uses this field to match an incoming SSO login to the correct Alianza account.
    - **IdP sign-in URL.** The SAML SSO endpoint of your IdP, which Alianza will redirect users to when they initiate an SSO login. This field is sometimes labeled as the SSO URL, SAML Endpoint, or Identity Provider Login URL.
    - **Sign-in Public Key.** The public key certificate (PEM or CER file) used to verify the authenticity of SAML assertions sent from your IdP to Alianza, ensuring login requests are legitimate and have not been tampered with.
6. Click **[Save]**. If all fields are complete, the status is updated to *Ready*.

© 2026 Cymbus, Inc.

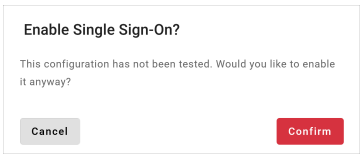


7. Locate the configuration in the list and, if it's in a **Ready** status, click **Test** on the right.
   - **Successful.** The SSO configuration is ready to be enabled.
   - **Unsuccessful.** One or more fields were entered incorrectly. Check your settings and try again.



Enable SSO Configuration

1. Locate the configuration to be enabled and switch the *Enable* toggle on.
2. If testing has not been completed, a confirmation message will appear. Read the message, then click **[Cancel]** to go back and test the configuration before it's enabled or click **[Confirm]** to proceed.



3. All users on the account now use this authentication method to log in.
4. Notify the account users that they must sign in using SSO from now on. This part is important because there will be no visual indication on the login page that the process has

© 2026 Cymbus, Inc.

changed. If they enter their username and password, they will get an error and will be unable to reset their password.

For an example notification, see Customer Notification Templates.

Switch SSO Configurations

Follow these steps to switch which SSO configuration is enabled on the account.

1. Add a new SSO configuration and test it to make sure it works.
2. Disable the current configuration by switching the **Enable** toggle off.
3. For the new configuration you want to enable, switch the **Enable** toggle on. Customers will now use this SSO authentication method.
4. Notify your customers that their SSO authentication method has been switched, so they will need to use their credentials for the new IdP to log in.

Disable SSO Configuration

To disable SSO and go back to using local authentication (username and password) to log in, switch the **Enable** toggle off. Remember to notify the account users that they will need to reset their password to log in.

Customer Notification Templates

Alianza does not email your customers when the authentication method is changed, so it's important for you to let them know what's going on. Feel free to use these email templates to communicate with your customers — just remember to customize them with your information first.

Subject	Email Body
SSO Enabled	Hi <First Name>, Single sign-on (SSO) has been enabled for your <Title> account. This means you no longer need to remember a separate username and password for this service and will sign in with your <Identity Provider's> credentials instead. To access the portal or the UC app, click **[Sign in with SSO]** and enter your <Identity Provider's> credentials. Thank you, <Signature>

© 2026 Cymbus, Inc.

Subject	Email Body
SSO Disabled	Hi <First Name>, Single sign-on (SSO) has been disabled for your account, which means you will no longer sign in using your <Identity Provider's> credentials. The next time you log in to the portal or UC app, click **[Forgot password?]** on the login screen to update your password. Thank you, <Signature>

© 2026 Cymbus, Inc.

Copyright © 2026. Alianza, LLC.

All rights reserved.