

# Linkus Server Admin Guide

Yeastar P-Series Software Edition

Version:

Date: 2024-07-05



# Contents

|  |           |
|--|-----------|
| <b>Linkus Overview.....</b>  | <b>1</b>  |
| <b>Linkus Server.....</b>  | <b>5</b>  |
| Set up Linkus Server with Remote Access Service.....   | 5         |
| Manually Set up Linkus Server.....   | 8         |
| Configure Linkus Client Login Mode.....  | 13        |
| Configure Audio Codec for Linkus Mobile Client.....  | 14        |
| Enable or Disable ICE (Interactive Connectivity Establishment) for Linkus Mobile Client..... | 16        |
| Configure Linkus Welcome Email.....  | 18        |
| <b>Linkus Client.....</b>  | <b>20</b> |
| Enable or Disable Linkus Clients for a User.....   | 20        |
| Set up User Permissions of Linkus Clients.....   | 21        |
| Send Linkus Client Login Credentials to Users.....   | 24        |

# Linkus Overview

Yeastar Linkus is designed to keep users connected with colleagues, business partners, and customers anywhere and anytime. To help you quickly understand how to set up and use Yeastar Linkus, we provide an overview on it, including information on Linkus server, Linkus clients, and Linkus event notifications.

## Linkus server

You need to configure Linkus server according to the users' needs for using Linkus.

- If users only need to use Linkus within the company's Local Area Network (LAN), you need to complete the following settings on Linkus Server:
  - [Enable Linkus clients for users](#)
  - [Send Linkus login credentials to users](#)
- If users need to use Linkus outside the company, you should set up Linkus server for remote access. Yeastar P-Series Software Edition provides the following two remote working solutions to help you set up a remote Linkus server.

### Remote Access Service (RAS)

**Remote Access Service** is a subscription-based service designed for remote working, which is included in **Enterprise Plan** and **Ultimate Plan**.

After you subscribe to the plan to get Remote Access Service, you can bind a Yeastar FQDN to the PBX, and enjoy the following benefits:

- Secure connection
- Network Address Translation (NAT) for Linkus service auto configured
- Linkus server for remote access auto configured
- Remote access to Linkus Web Client, Desktop Client and Mobile Client
- Advanced Linkus features, such as Instant Messaging (IM), video call and video conferencing

If you choose this solution, refer to the following topics to complete the setup.

- [Set up Linkus server with Remote Access Service](#)
- [Enable Linkus clients for users](#)
- [Send Linkus login credentials to users](#)

### Manual configuration

If you don't subscribe to **Remote Access Service** and users need to use Linkus in external network, you have to go through complicated server and network settings, such as port forwarding, NAT and public IP address configuration, so as to implement remote access to Linkus.



**Note:**

- Weak network protection will cause SIP attacks.
- Incorrect configurations may cause one-way audio issue.
- Linkus server that is manually configured does NOT support remote access to Linkus Web Client, and the features of Instant Messaging (IM), video call and video conferencing.

If you choose this solution, refer to the following topics to complete the setup.






- [Manually set up Linkus server](#)
- [Enable Linkus clients for users](#)
- [Send Linkus login credentials to users](#)




## Linkus client

### Linkus client types

Yeastar P-Series Software Edition supports Linkus Mobile Client, Desktop Client, and Web Client.

The following table lists the requirements for using Linkus clients, as well as the corresponding download links and user guides.

| Linkus Client  |   | Requirement   |
|--|---|---|
|  <b>Linkus Mobile Client</b>  |  <a href="#">iOS</a>     | <ul style="list-style-type: none"> <li>• iOS 11.0 or later</li> </ul>   |
|  |  <a href="#">Android</a> | <ul style="list-style-type: none"> <li>• Android 6.0 or later</li> </ul>  |
|  <b>Linkus Desktop Client</b> |  <a href="#">Windows</a> | <ul style="list-style-type: none"> <li>• Windows 7 or later</li> <li>• Minimum 2 GHz (32-bit or 64-bit) processor</li> <li>• Minimum 4 GB memory</li> <li>• Minimum 300 MB free hard drive space</li> </ul> |

| Linkus Client  |   | Requirement  |
|--|---|--|
|  |  macOS   | <ul style="list-style-type: none"> <li>• OS X 10.11 El Capitan or later</li> </ul>   |
|  <b>Linkus Web Client</b> |  Browser | <ul style="list-style-type: none"> <li>• Google Chrome 87 or later</li> <li>• Microsoft Edge 87 or later</li> <li>• Opera 72 or later</li> </ul> |

## Linkus client user permissions

By default, users can access all the menus and configure all the settings within Linkus clients. You can set up permission rules to restrict users' access and configuration permission:

- **Menu Visibility Permission:** Restrict users from specific menus within Linkus clients.
- **Operation Permission:** Restrict users from specific settings within Linkus clients.

For more information, see [Set up User Permissions of Linkus Clients](#).

## Linkus client login methods

Yeastar P-Series Software Edition allows users to log in to Linkus clients using different methods, including quick login via a login link or QR code, and manual login with login information.

### Quick login

You can send login credentials to users via Linkus welcome emails. In this way, the users can quickly and easily log in to Linkus clients with the QR code or login link provided in the email.

For more information, see [Send Linkus Welcome Emails to Users for Quick Login](#).

### Manual login

In case users fail to receive Linkus welcome emails or access their mailboxes, you can provide login information (the username and password of extension account as well as Linkus server network information) for users. In this way, users can manually enter the login information and log in to Linkus clients.

For more information, see [Send Linkus Login Information to Users for Manual Login](#).

## Linkus events

Yeastar P-Series Software Edition provides event notification feature. When the following Linkus events occur, the system will record events in logs and notify relevant contacts via specific notification methods.

| Event                           | Description  |
|---------------------------------|--|
| <b>Operations-related event</b> |  |
| Web User Login Success          | An extension user successfully logged in to Linkus Web Client.   |
| Web User Login Failed           | An extension user failed to log in to Linkus Web Client.   |
| Linkus Client Login Failed      | An extension user failed to log in to Linkus Mobile Client or Linkus Desktop Client.   |
| Extension User Password Changed | An extension user's user password was changed.   |
| <b>Security-related event</b>   |  |
| Web User Blocked Out            | A specific source IP address was blocked by the system due to too many failed login attempts to Linkus Web Client.                             |
| Linkus User Blocked Out         | A specific source IP address was blocked by the system due to too many failed login attempts to Linkus Mobile Client or Linkus Desktop Client. |

You can customize the event level, notification email template or manage relevant contacts on **System > Event Notification**. For more information, see [Configure Event Notifications](#) and [Manage Notification Contacts](#).

# Linkus Server

## Set up Linkus Server with Remote Access Service

After you get Remote Access Service, users can remotely access Linkus Mobile Client using the PBX Serial Number (SN). To allow remote access to Linkus Desktop Client and Linkus Web Client, you need to further configure a Yeastar-supplied Fully Qualified Domain Name (FQDN) on the system.

### Procedure

1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
  - a. Select a domain name from the drop-down list.
  - b. Enter a host name in the first field.



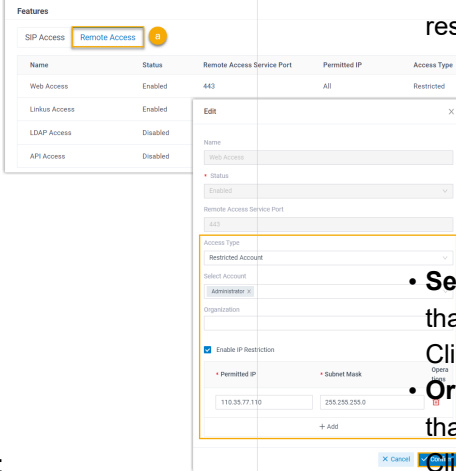



#### Note:

Think twice before you enter the hostname. The FQDN can not be changed after you save the configurations.

For example, select domain name **ras.yeastar.com** and enter host name `yeastardocs`. You will get an FQDN **yeastardocs.ras.yeastar.com**.

4. **Optional:** Configure the remote access permission according to your need.

| Remote Access Permission                               | Instruction  |
|--|--|
| Figure 1.<br><b>Configure remote access permission</b> | By default, all extension accounts are allowed to access Linkus Web Client via FQDN. You can change the remote access permission as needed. <ol style="list-style-type: none"><li>a. In the <b>Features</b> section, go to the <b>Remote Access</b> tab.</li></ol> |

| Remote Access Permission   | Instruction   |
|--|---|
| <div>for Linkus Web Client</div> <div></div> <div>t</div> | <div><div>b. Click  beside the <b>Web Access</b> feature.</div><div>c. In the pop-up window, set up the access permission:<ul style="list-style-type: none"><li>• <b>Access Type</b>: Define the account access restriction type.<ul style="list-style-type: none"><li>◦ <b>Allowed Account</b>: Only the selected accounts can remotely access Linkus Web Client.</li><li>◦ <b>Restricted Account</b>: All accounts except for the selected accounts can remotely access Linkus Web Client.</li></ul></li><li>• <b>Select Account</b>: Select the desired accounts that can or can not remotely access Linkus Web Client.</li><li>• <b>Organization</b>: Select the desired organization(s) that can or can not remotely access Linkus Web Client.</li></ul></div><div><div><b>Note:</b><br/>This setting is available only when the <b>Organization Management</b> feature is enabled.</div><ul style="list-style-type: none"><li>• <b>Enable IP Restriction</b>: Select the checkbox of the option, and add at least one permitted IP address and subnet mask.<br/><br/>If you configure this option, only the devices with the permitted IP address(es) can remotely access Linkus Web Client.</li></ul></div><div>d. Click <b>Confirm</b>.</div></div> |
| <div>Figure 2. <b>Configure remote access permission for Linkus Desktop Client and Mobile</b></div>  | <div>You can set IP restriction rules for remote access to Linkus Desktop Client and Mobile Client. In this way, users can only remotely access Linkus Mobile Client and Desktop Client on the devices with the permitted IP address(es).</div> <div><div>a. In the <b>Features</b> section, go to the <b>Remote Access</b> tab.</div><div>b. Click  beside the <b>Linkus Access</b> feature.</div><div>c. Select the checkbox of <b>Enable IP Restriction</b>, then add at least one permitted IP address and subnet mask.</div></div>  |



| Remote Access Permission           | Instruction                            |
|------------------------------------|--|
| <p><b>Clie</b></p> <p><b>t</b></p> | <p><b>d. Click <b>Confirm</b>.</b></p> |

5. Click **Save**.

## Result

- Linkus server is automatically set up for remote access with the FQDN. The following information is displayed on the **Linkus Server** page:

Remote Access Service

Status

Connected

Domain Name

yeastardocs.ras.yeastar.com

- **Status:** Connected, which means that Linkus server is set up successfully.
- **Domain Name:** The domain name can be used for Linkus remote access.
- Users can use Linkus (Mobile Client, Desktop Client, and Web Client) via the FQDN remotely.

## What to do next

- [Configure Linkus Client Login Mode](#)
- [Enable or Disable Linkus Clients for a User](#)
- [Send Linkus Client Login Credentials to Users](#)

# Manually Set up Linkus Server

This topic describes how to manually set up Linkus server according to different network scenarios.

## Restrictions



### Important:

- Manually configured Linkus server does NOT support remote access to Linkus Web Client. To allow users to access and use Linkus Web Client remotely, you need to set up Linkus server with **Remote Access Service (RAS)**.

For more information, see [Set up Linkus Server with Remote Access Service](#).

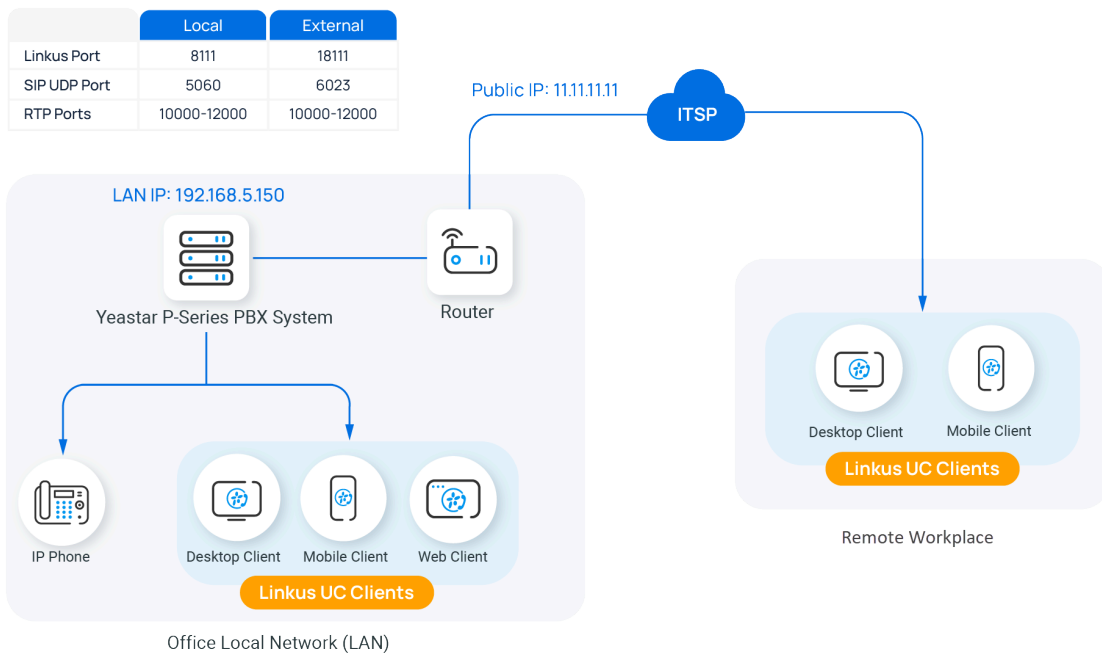
- Manually configured Linkus server does NOT support the features of Instant Messaging (IM), video call and video conferencing.

## Network scenarios

- [PBX is behind a router](#)
- [PBX is connected to the ISP router directly](#)
- [PBX is connected to a VPN network](#)

### PBX is behind a router

If your PBX is behind a router and Linkus communicates with the PBX through the network interface that is configured with a private IP, you need to forward Linkus-related ports on your router and configure SIP NAT settings on your PBX.



## Procedure

Based on the above network topology, you can configure Linkus server and your router as follows:

1. Check the following local service port on your PBX system (Path: **System > Network > Service Ports**), and forward the ports on your router.

In this example, check and forward the following ports:



### Important:

To ensure that RTP packets can be transmitted correctly, the same RTP ports should be used both inside and outside of the network. You can check and modify the RTP port range on **PBX Settings > SIP Settings > General > Basic > RTP Port Range**.

| Service Port                        | Local Port   | External Port |
|-------------------------------------|--------------|---------------|
| Linkus Port                         | TCP&UDP 8111 | TCP&UDP 18111 |
| SIP UDP Port (for SIP registration) | UDP 5060     | UDP 6023      |

| Service Port | Local Port      | External Port   |
|--------------|-----------------|-----------------|
| RTP Ports    | UDP 10000-12000 | UDP 10000-12000 |

2. Configure SIP NAT on your PBX for remote access.

The SIP NAT settings should be configured to ensure that SIP data can be transmitted correctly between the PBX and the public Internet.

The screenshot shows the 'Public IP (NAT)' configuration interface. It includes a 'NAT Type' dropdown set to 'Public IP Address', a 'Public IP Address' field with '11.11.11.11', and a 'Local Network Identification' section with a table for 'Network Number' (192.168.5.0) and 'Subnet Mask' (255.255.255.0). There is an '+ Add IP' button and an 'Operations' column with a trash icon. The 'NAT Mode' is set to 'Yes'.

- Log in to PBX web portal, go to **System > Network > Public IP and Ports**.
  - Turn on **Public IP (NAT)**.
  - In the **NAT Type** drop-down list, select **Public IP Address**.
  - In the **Public IP Address** field, enter the public IP address. In this example, enter **11.11.11.11**.
  - In the **Local Network Identification** section, click **+ Add IP** to add all your local network. In this example, enter **192.168.5.0/255.255.255.0**.
  - In the **NAT Mode** drop-down list, select **Yes**.
3. In the **Public Ports** section, enter external SIP port and Linkus service port, which helps the router to direct appropriate traffic from the Internet to the PBX.

The screenshot shows the 'Public Ports' configuration interface. It has two columns of input fields. The left column contains 'External SIP UDP Port' (6023), 'External SIP TLS Port', and 'External Web Server Port'. The right column contains 'External SIP TCP Port', 'External Linkus Port' (18111), and 'External LDAP Port'. The 'External SIP UDP Port' and 'External Linkus Port' fields are highlighted with orange boxes.

- **External SIP UDP Port:** In this example, enter **6023**.
- **External Linkus Port:** In this example, enter **18111**.

4. Click **Save** and **Apply**.

## Result

Linkus server for both local access and remote access is set up.

**Note:**

When users use Linkus within company's Local Area Network (LAN), Linkus communicates through the local IP address. Otherwise, Linkus communicates through the external IP address.

## What to do next

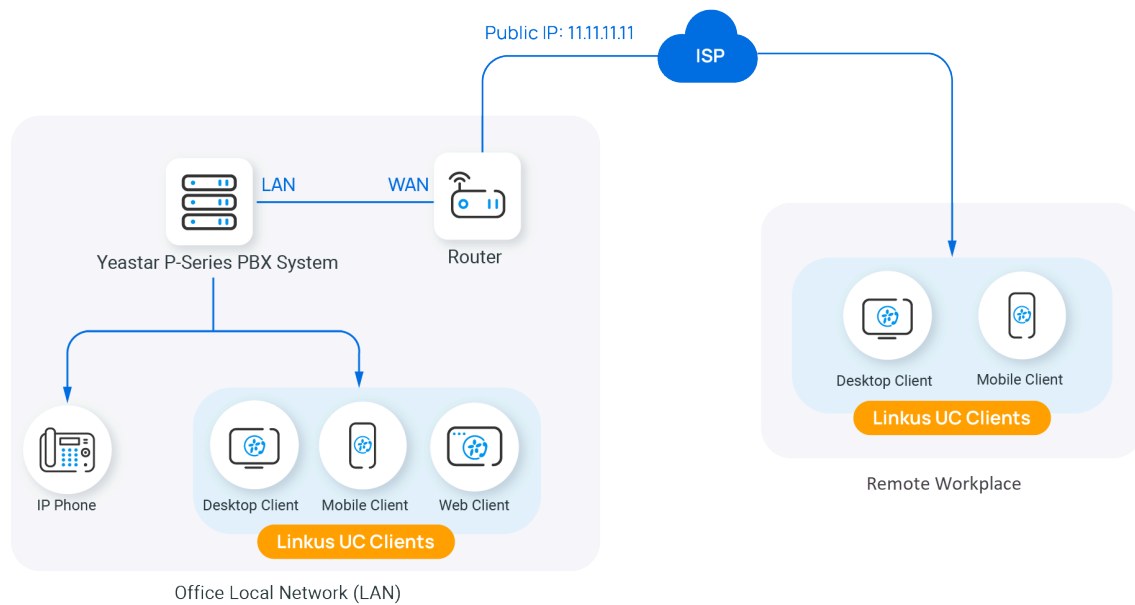
- [Configure Linkus client login mode](#)
- [Enable Linkus clients for users](#)
- [Send Linkus client login credentials to users](#)

## PBX is connected to the ISP router directly

If the PBX is connected to an Internet Service Provider (ISP) router, the Linkus server is ready to be accessed remotely.

**Note:**

- In this network scenario, you do NOT need to do port forwarding on your router and configure SIP NAT settings on your PBX.
- In this network scenario, we recommend that you change the default SIP UDP port on the PBX to improve the system security (Path: **PBX Settings > SIP Settings > General > Basic > SIP UDP Port**).



## What to do next

- [Configure Linkus client login mode](#)
- [Enable Linkus clients for users](#)
- [Send Linkus client login credentials to users](#)

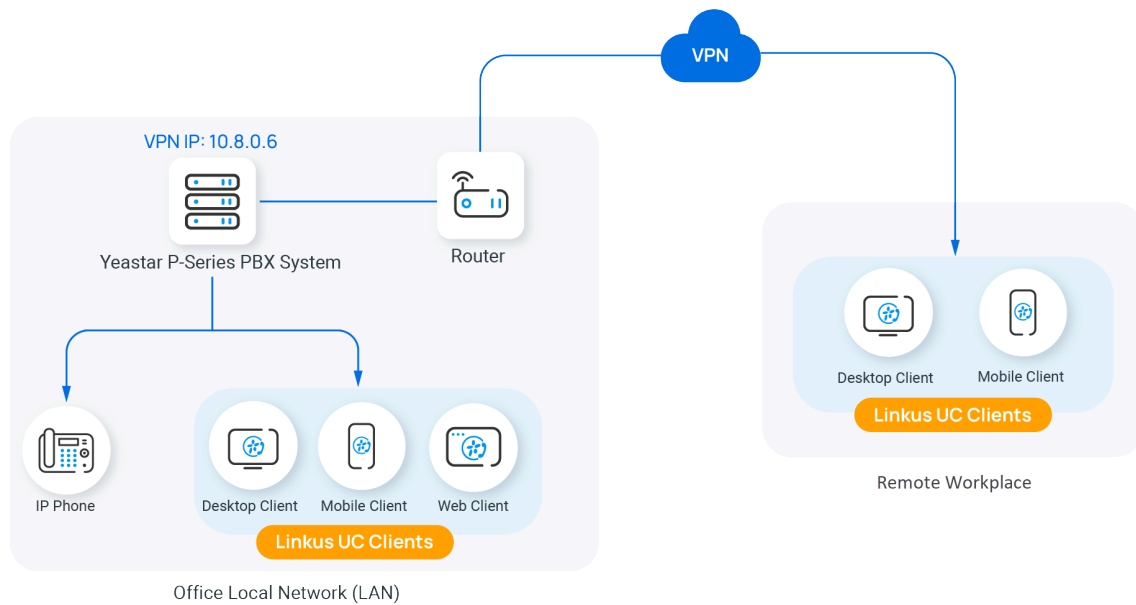
## PBX is connected to a VPN network

If your PBX is connected to a VPN network, the Linkus server is ready to be accessed by the VPN network.



### Note:

In this network scenario, you do NOT need to do port forwarding on your router or configure SIP NAT settings on your PBX.



## What to do next

- [Configure Linkus client login mode](#)
- [Enable Linkus clients for users](#)
- [Send Linkus client login credentials to users](#)

# Configure Linkus Client Login Mode

Yeastar P-Series Software Edition supports two login modes for Linkus clients. You can decide how users can manually log in to Linkus clients.

## Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. At the top of the extension list, click **Linkus Server**.
3. In the **Linkus Client Login Mode** section, select the checkboxes of the desired login modes.
  - **Extension Number:** Users can use extension number as the username for Linkus login.
  - **Email Address:** Users can use the email addresses that are bound with their extensions as the username for Linkus login.
4. Click **Save**.

# Configure Audio Codec for Linkus Mobile Client

Yeastar P-Series Software Edition provides multiple codecs for users to adjust audio quality of calls on Linkus Mobile Client. You can configure global settings of codec for Linkus Mobile Client, or customize the codec setting for different users based on their needs.

**Note:**

This topic shows you how to configure audio codec for Linkus Mobile Client on PBX web portal. Extension users can also change the codec setting on their Linkus Mobile Clients (Path: **Account > Settings > Audio Options > Codec**), and the updated setting will be automatically synchronized to the PBX.

## Requirements

- **PBX Server:** Version 83.15.0.22 or later
- **Linkus Mobile Client:**
  - **Linkus iOS Client:** Version 5.5.9 or later
  - **Linkus Android Client:** Version 5.5.8 or later

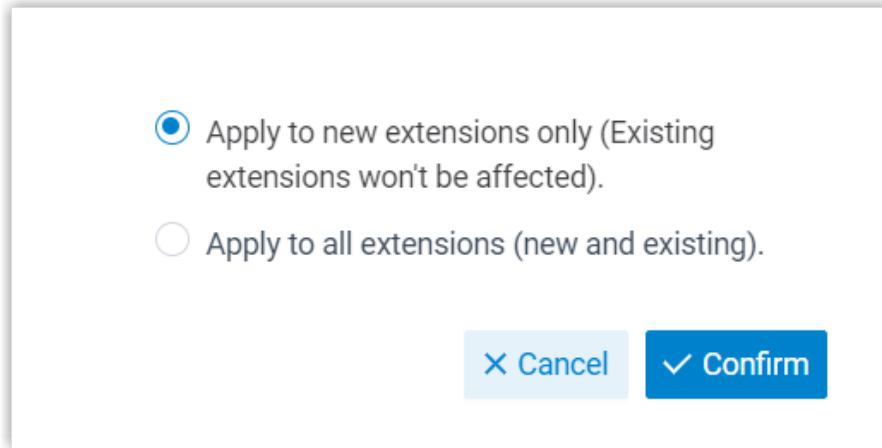
## Configure codec for all users' Linkus Mobile Client (global setting)

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. At the top of the extension list, click **Linkus Server**.
3. In the **Linkus Mobile Default Settings** section, complete the following settings.
  - a. In the **Linkus Mobile Client Codec** drop-down list, select an audio codec.

The screenshot shows the 'Linkus Mobile Default Settings' page. Under the 'Linkus Mobile Client Codec' section, there is a dropdown menu. The menu is open, showing a list of available codecs: 'u-law', 'a-law', 'iLBC', 'G722', and 'G729'. The 'u-law' option is currently selected and highlighted in light blue.



- b. Click **Save**.
- c. In the pop-up window, set whether to apply the codec setting to new extensions only or to all extensions (new and existing), then click **Confirm**.




☒ Apply to new extensions only (Existing extensions won't be affected).

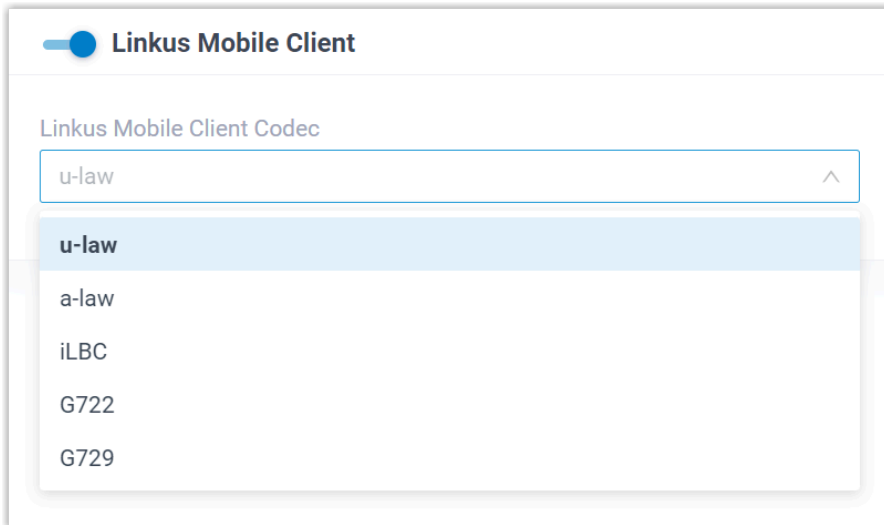
☐ Apply to all extensions (new and existing).

✕ Cancel ✓ Confirm

The codec setting is synchronized to extension users' Linkus Mobile Client and takes effect immediately.

## Configure codec for a user's Linkus Mobile Client (specific setting)

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click  beside the desired extension user, then go to the **Linkus Clients** tab.
3. In the **Linkus Mobile Client Codec** drop-down list, select an audio codec.



☒ **Linkus Mobile Client**

Linkus Mobile Client Codec

u-law

u-law  
 a-law  
 iLBC  
 G722  
 G729

4. Click **Save**.

The codec setting is synchronized to the extension user's Linkus Mobile Client and takes effect immediately.

## Enable or Disable ICE (Interactive Connectivity Establishment) for Linkus Mobile Client

ICE (Interactive Connectivity Establishment) is a technique used to establish direct connections between Yeastar PBX and Linkus, improving call quality by reducing network latency and packet loss. You can configure global ICE settings for Linkus Mobile Client, or customize the ICE setting for different users based on their needs.



### Note:

This topic shows you how to configure ICE setting for Linkus Mobile Client on PBX web portal. Extension users can also change the ICE setting on their Linkus Mobile Clients (Path: **Account > Settings > Audio Options > ICE**), and the updated setting will be automatically synchronized to the PBX.

### Requirements

- **PBX Server:** Version 83.15.0.22 or later
- **Linkus Mobile Client:**
  - **Linkus iOS Client:** Version 5.5.9 or later
  - **Linkus Android Client:** Version 5.5.8 or later

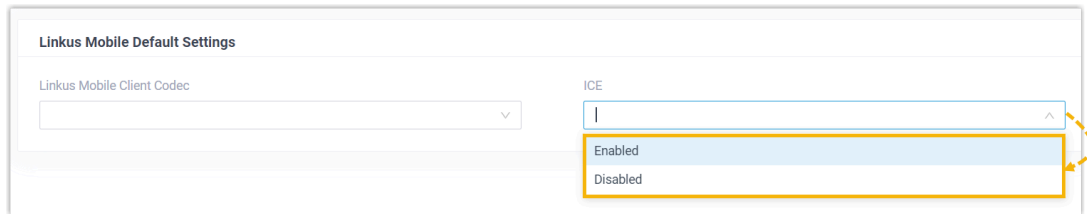
### Configure ICE for all users' Linkus Mobile Client (global setting)

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. At the top of the extension list, click **Linkus Server**.
3. In the **Linkus Mobile Default Settings** section, complete the following settings.
  - a. In the **ICE** drop-down list, select an option.



### Note:

If you disable ICE, video calls will be unavailable on users' Linkus Mobile Client.



Linkus Mobile Default Settings

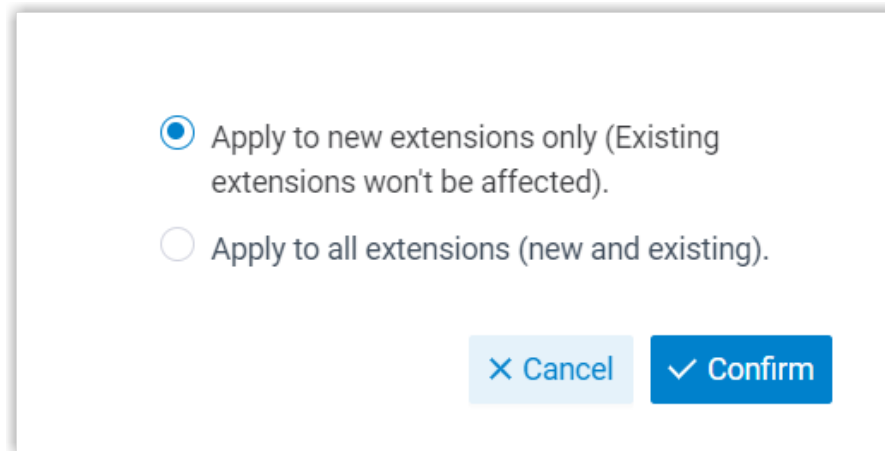
Linkus Mobile Client Codec

ICE

Enabled

Disabled

- b. Click **Save**.
- c. In the pop-up window, set whether to apply the ICE setting to new extensions only or to all extensions (new and existing), then click **Confirm**.



☒ Apply to new extensions only (Existing extensions won't be affected).


☐ Apply to all extensions (new and existing).

✕ Cancel

✓ Confirm

The ICE setting is synchronized to extension users' Linkus Mobile Client, and will take effect when extension users quit and reopen the APP or re-login to the APP.

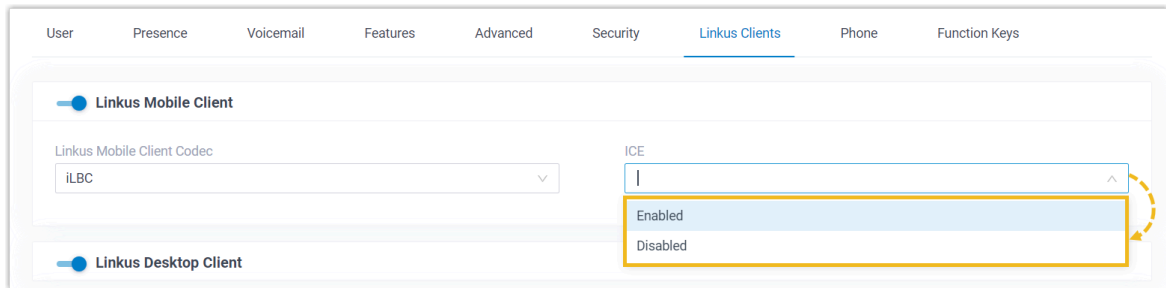
### Configure ICE setting for a user's Linkus Mobile Client (specific setting)

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click  beside the desired extension user, then go to the **Linkus Clients** tab.
3. In the **ICE** drop-down list, select an option.



**Note:**

If you disable ICE, video calls will be unavailable on the user's Linkus Mobile Client.



4. Click **Save**.

The ICE setting is synchronized to the extension user's Linkus Mobile Client, and will take effect when the extension user quits and reopens the APP or re-logs in to the APP.

## Configure Linkus Welcome Email

Linkus welcome email is used to provide users with their extension number and voicemail PIN, as well as the login credentials and instructions of all Linkus clients. Yeastar P-Series Software Edition provides a default email template, you can also customize your own template.



**Note:**

By default, Yeastar P-Series Software Edition sends Linkus welcome emails in the language that you have set in system email template (Path: **System > Email > Email Templates > Notification Email Language**).

### Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. At the top of the extension list, click **Linkus Server**.
3. Click **Email Templates** tab.
4. Customize email template.
  - a. In the **Template** drop-down list, select **Custom**.
  - b. Edit email subject and content according to your needs.



**Important:**

Do NOT change the variables `{{ .xxx }}` in the email template, otherwise the information in Linkus welcome emails would be wrong.

c. Click **Save**.

**Related information**

[Send Linkus welcome emails to users for quick login](#)


# Linkus Client

## Enable or Disable Linkus Clients for a User

Users can use Linkus only if the Linkus clients are enabled for their extension accounts. You can enable or disable Linkus clients for users as needed.

### Enable Linkus clients for a user

#### Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click  beside the desired extension.
3. Click **Linkus Clients** tab.
4. Turn on the switch of the desired Linkus client(s).
5. Click **Save** and **Apply**.

#### Result


Users can log in to Linkus clients that are enabled with their Linkus client login credentials.

#### What to do next

- [Set up User Permissions of Linkus Clients.](#)
- [Send Linkus Client Login Credentials to Users.](#)

### Disable Linkus clients for a user

#### Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click  beside the desired extension.
3. Click **Linkus Clients** tab.
4. Turn off the switch of the desired Linkus client(s).
5. Click **Save** and **Apply**.

#### Result

The user can NOT log in to and use the Linkus client that has been disabled.

## Set up User Permissions of Linkus Clients

After enabling Linkus clients for users, they can access all the menus and configure all the settings within Linkus clients. You can set up permission rules to specify the menus and settings that users can access and configure, which will be applied to all the Linkus clients.

### Requirements

| Server / Client       | Version Requirement  |
|-----------------------|--|
| PBX Server            | Version 83.12.0.57 or later  |
| Linkus Desktop Client | <ul style="list-style-type: none"> <li>• <b>Windows Desktop:</b> Version 1.2.14 or later</li> <li>• <b>Mac Desktop:</b> Version 1.2.10 or later</li> </ul>             |
| Linkus Mobile Client  | <ul style="list-style-type: none"> <li>• <b>Linkus iOS Client:</b> Version 5.2.9 or later</li> <li>• <b>Linkus Android Client:</b> Version 4.13.16 or later</li> </ul> |

### Set up menu visibility permission


By default, users can access all the menus within Linkus clients. You can set up menu visibility to restrict users from specific menus.

#### Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Menu Visibility**.

The default rule that allows all users to access all the menus is displayed on the list.

2. Click **Add rule**.
3. Customize an access rule for menus, then click **Save**.

- **Extension/Extension Group:** Click  to select desired extensions, extension groups, or departments.

- **Permission Type:** Select an option from the drop-down list to define the permission.
  - **Allow use:** Allow to access specific menus within Linkus clients.
  - **Disallow use:** Disallow to access specific menus within Linkus clients.
- **Menu:** Select the menus that are allowed or disallowed to be accessed.

## Result

The rule takes effect immediately. Users can only view and access the menus that are visible to them on Linkus clients.

## Set up operation permission

By default, extension users can configure all the settings within Linkus clients. You can set up operation permission to specify the settings that users can configure or modify.


## Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Preference Settings**.

The default rule that allows all users to configure all the settings is displayed on the list.

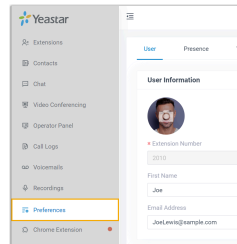
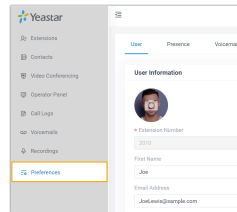
2. Click **Add rule**.
3. Customize a rule for settings, then click **Save**.

The screenshot shows the 'Add rule' dialog box in the 'Operations' tab. The dialog has four columns: 'Extension/Extension Group', 'Permission Type', 'Configuration Item', and 'Operations'. The 'Add rule' button is highlighted with a blue dashed box. Below it, a row is being edited, with the 'Save' button highlighted by a red dashed arrow.

- **Extension/Extension Group:** Click  to select desired extensions, extension groups, or departments.
- **Permission Type:** Select an option from the drop-down list to define the permission.
  - **Allow edit:** Allow to configure specific settings of Linkus clients.



- **Disallow edit:** Disallow to configure specific settings of Linkus clients.
- **Configuration Item:** Select the settings that are allowed or disallowed to be configured.  
Refer to the table below for the configuration items on Linkus clients controlled by each option.

| Option              | Linkus Mobile Client   | Linkus Web Client   | Linkus Desktop Client                                     |
|---------------------|--|---|---|
| User                | Settings in <b>Account &gt; Personal Information</b> (controlled by the option <b>User Information</b> ).  | <p>Settings in the corresponding tab in the <b>Preferences</b> menu.</p> <p>Figure 3.<br/><b>Linkus Web Client</b></p>  <p>Figure 4.<br/><b>Linkus Desktop Client</b></p>  |   |
| Presence            | Settings in <b>Account &gt; Current Presence</b> .   |   |   |
| Voice mail          | /  |   |   |
| Audio & Video       | /  |   |   |
| Features            | The following configuration items in <b>Account &gt; Settings &gt; Advanced</b> : <ul style="list-style-type: none"><li>◦ <b>Call Waiting</b> feature (controlled by the option <b>Call</b>).</li><li>◦ Settings of <b>Switch Business Hours Status</b> feature (controlled by the option <b>Time-conditional Presence Auto Switch</b>).</li></ul> |   |   |
| Function Keys       | /  |   |   |
| Outlook Integration | /  | /   | Settings in <b>Preferences &gt; Outlook Integration</b> . |

| Option                     | Linkus Mobile Client   | Linkus Web Client  | Linkus Desktop Client |
|----------------------------|--|--|-----------------------|
| Change Password & Security | <b>Password Management</b> feature in <b>Account &gt; Settings</b> (controlled by the option <b>Change Password</b> ). | Settings in <b>Account &gt; Change Password &amp; Security</b> . |                       |

## Result

The rule takes effect immediately. Users can only configure the settings that they are allowed to configure on Linkus clients.

# Send Linkus Client Login Credentials to Users

After you enable Linkus clients for users, you need to send login credentials to them. This topic describes what information you need to provide, and how users can login with the provided information.

## Send Linkus welcome emails to users for quick login

In most cases, you can send Linkus welcome emails to users, so that they can quickly log in to Linkus clients with the login QR code or login link provided in the email.

## Prerequisites

- **System configuration**

- Make sure that Linkus server has been set up.

For more information about the configurations, see [Set up Linkus Server with Remote Access Service](#) or [Manually Set up Linkus Server](#).

- Make sure that the [system email server](#) works.

- **Extension configuration**

- You have configured email addresses for the desired extensions.
- You have [enabled at least one Linkus client for the desired extensions](#).

## Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Select the checkbox(es) of the desired extension(s), then click **Welcome Email** at the top of the extension list.

## Result

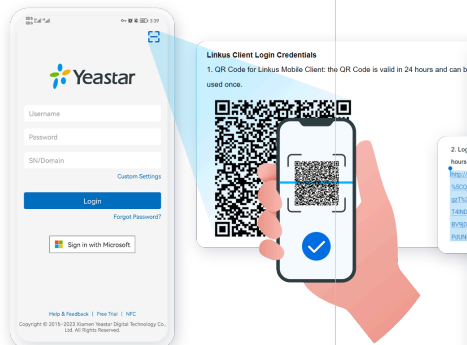
The specified users will receive the Linkus welcome emails. They can use the QR code or the login link to log in to their Linkus clients as the following figures show.



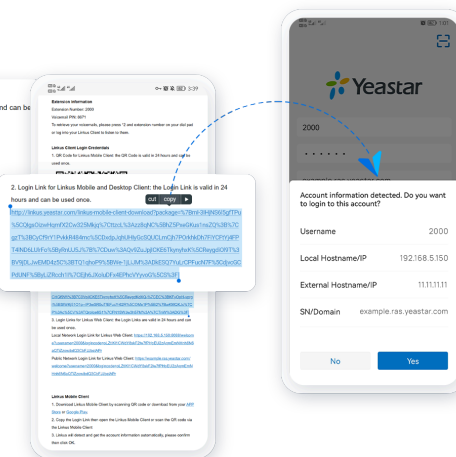
### Note:

The QR code and login link are valid in 24 hours and can only be used once.

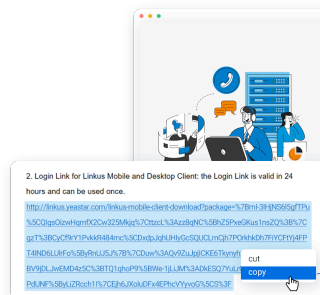
**Figure 5. Mobile Client Quick Login (QR Code)**



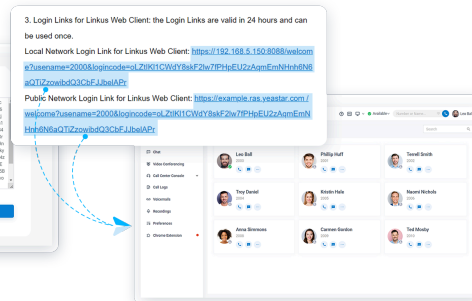
**Figure 6. Mobile Client Quick Login (Login Link)**



**Figure 7. Desktop Client Quick Login (Login Link)**



**Figure 8. Web Client Quick Login (Login Link)**



## Send Linkus login information to users for manual login

In case users fail to receive Linkus welcome emails or access their mailboxes, you can provide users with the username and password of their extension accounts, as well as the network information of Linkus server, so that users can manually enter the login information to log in.

### Procedure

Provide different information for users based on the way you set up the Linkus server. Refer to the following table for the detailed login credentials.

| Linkus Server                               | Mobile & Desktop Login Credentials   | Web Client Login Credentials |
|---|--|------------------------------|
| Local Linkus Server                         | <ul style="list-style-type: none"> <li>• PBX's local IP address</li> <li>• Port               <ul style="list-style-type: none"> <li>◦ Local Linkus port (for Mobile &amp; Desktop Client)</li> <li>◦ Local web server port (for Web Client)</li> </ul> </li> <li>• Username (can be extension number or email address, depending on how you <a href="#">configure Linkus client login mode</a>)</li> <li>• Extension's user password</li> </ul> |                              |
| Remote Linkus Server (RAS)                  | <ul style="list-style-type: none"> <li>• <a href="#">The FQDN that is bound with the PBX</a>, or the PBX's serial number (for Mobile Client only)</li> <li>• Username (can be extension number or email address, depending on how you <a href="#">configure Linkus client login mode</a>)</li> <li>• Extension's user password</li> </ul>  |                              |
| Remote Linkus Server (Manual configuration) | <ul style="list-style-type: none"> <li>• PBX's local IP address and local Linkus port</li> <li>• PBX's public IP address/external host domain name and external Linkus port</li> <li>• Username (can be extension number or email address, depending on how you <a href="#">configure Linkus client login mode</a>)</li> <li>• Extension's user password</li> </ul>  | No supported.                |

### Result

Users can log in to Linkus clients by manually entering the information as the following figures show.

Figure 9. Mobile Client Manual Login (SN / FQDN)

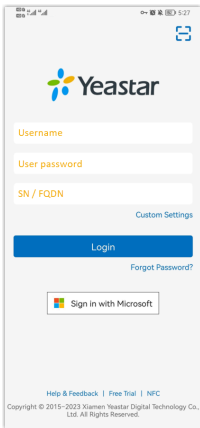


Figure 10. Mobile Client Manual Login (IP address & port)

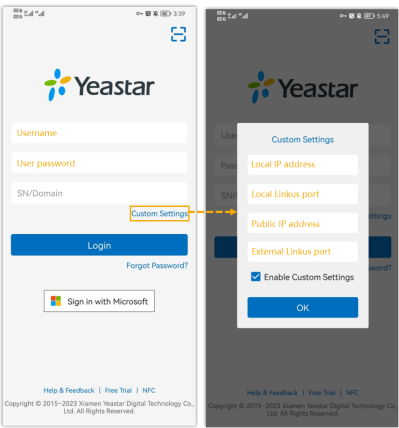


Figure 11. Desktop Client Manual Login (FQDN)

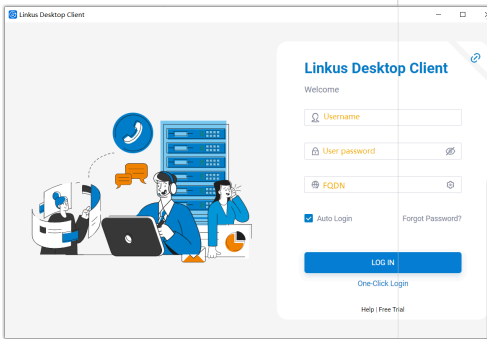


Figure 12. Desktop Client Manual Login (IP address & port)

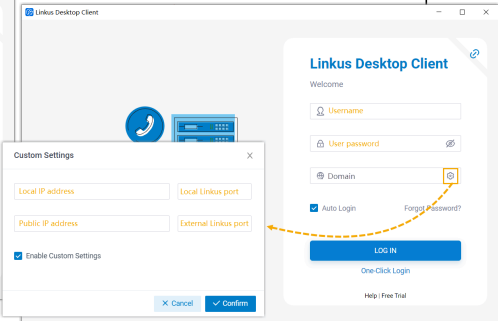


Figure 13. Web Client Manual Login (FQDN)

