

# Security Guide

Yeastar P-Series Appliance Edition

Version: 1.3

Date: 2025-12-10



# Contents

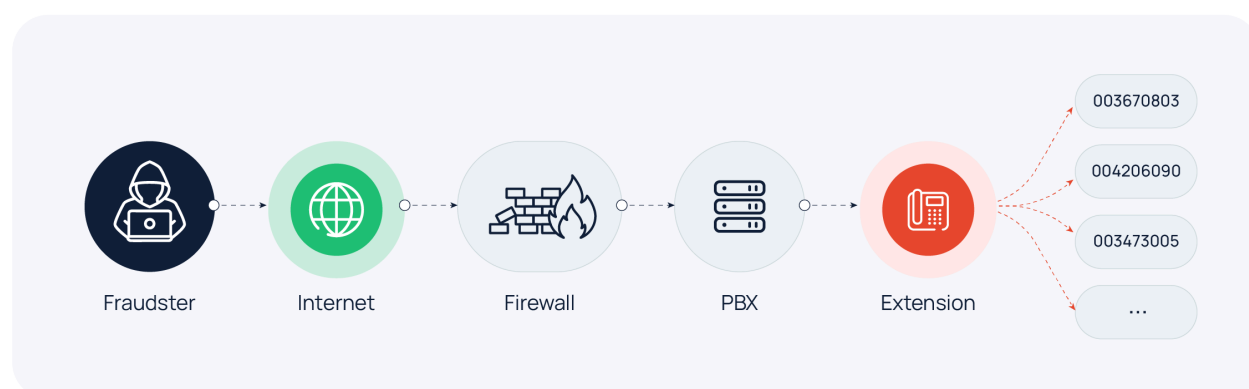
<b>Overview.....</b>	<b>1</b>
<b>System Security.....</b>	<b>3</b>
System Security.....	3
<b>Network Security.....</b>	<b>6</b>
Network Security.....	6
<b>Endpoint Security.....</b>	<b>12</b>
Extension Registration Security.....	12
Extension Login Security.....	17
<b>Outbound Call Security.....</b>	<b>26</b>
Outbound Call Security.....	26
<b>Contingency Plan.....</b>	<b>34</b>
Contingency Plan.....	34

# Yeastar P-Series PBX System Security Guide

Attacks on PBX system can come from the Internet or telephone lines. Fraudsters always try every means to exploit vulnerabilities to gain access to phone system and make fraudulent calls. As a result, fraudsters take revenues generated from these calls, while you get a costly telephone bill. The Security Guide is intended to elaborate on how to protect your PBX system from security breaches and mitigate the threat of toll fraud.

## How do fraudsters get access to a PBX?

Typically, fraudsters use vulnerability scanners to crawl the Internet looking for vulnerabilities in your company's firewalls (like open ports). If any open port is detected, the fraudsters may punch requests at the port in order to tease out information about system vulnerabilities. In the end, they may have all the information they need to brute force their way through the firewall. Once the firewall has been breached, the fraudsters can gain access to the PBX, build a back door into the system, and use it to route as much traffic as they want, eventually leading to toll fraud.



## How to protect PBX from security breaches and toll fraud?

Actually, vulnerabilities in your phone system can not be eliminated due to the ever-changing need of your business communications and ever-evolving of hacking techniques. However, you can reduce the vulnerabilities with better awareness, proactive actions, and regular audit.

To maintain a high level of security, we recommend that you adopt a multi-layered security strategy. This involves integrating several protective mechanisms to shield the system from

security threats. Even if one defense layer gets compromised, others remain in place to offer security.



# System Security

## System Security

System Security is the first line of defense in multi-layered security strategy, providing basic protection to shield your phone system from known threats and security breaches. You can enhance system security by **Upgrade Firmware**, **Disable Secure Shell (SSH)**, and **Change Default Ports**.

### Upgrade Firmware

Typically, the most recent firmware version is often the most secure with bugs and vulnerabilities being found and fixed. In addition, with technology evolving, some critical security features or layers of protection are only supported in the latest version. For security reasons, it is important to keep your PBX firmware up to date.

You can achieve this by scheduling automatic firmware upgrade whenever a new version is released.

1. Go to **Maintenance > Upgrade**.
2. In the **Automatic Upgrade** section, select **Check for updates and automatically install**, then specify the frequency and time as needed.



#### Note:

We recommend that you upgrade the system during non-business hours to avoid service interruption.

**Automatic Upgrade**

☐ Never check for updates

☐ Check for updates and notify me

☒ Check for updates and automatically install

\* Automatically check for updates at

Daily

\*

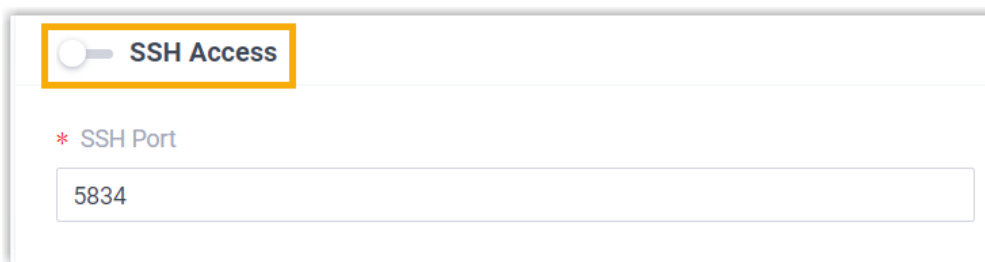
00:00

3. Click **Save** and **Apply**.

## Disable Secure Shell (SSH)


Hackers are constantly scanning for SSH servers and repeatedly trying thousands of username and password combinations in seconds until gaining access to the server. Once the hackers gain access, they can get valuable information for toll fraud or other malicious purposes. To prevent this, we recommend that you disable SSH for PBX system and enable SSH ONLY when troubleshooting is required.

To disable SSH, go to **Security > Security Settings > Console/SSH Access**, turn off the switch of **SSH Access**.



## Change default ports

Port scanning is a popular method used by fraudsters to identify open ports that can be exploited to break into phone systems. Standard ports, such as port 5060, are often targeted by fraudsters. It is therefore advisable to change the default ports to non-standard ports if your PBX is exposed to the Internet, as shown below.

1. Go to **System > Network > Service Ports**.
2. Click  to beside the desired service port.

System / Network

Basic Settings

Web Server

Service Ports

Yeastar FQDN

Public IP and Ports

Static Routes

DHCP Server

HTTPS

SIP UDP

SIP TLS

RTP

SSH

Database Grant

FTP

HTTP

SIP TCP

Outbound SIP Port

Linkus

AMI

LDAP Port

TFTP

3. Change the default port and save the setting.

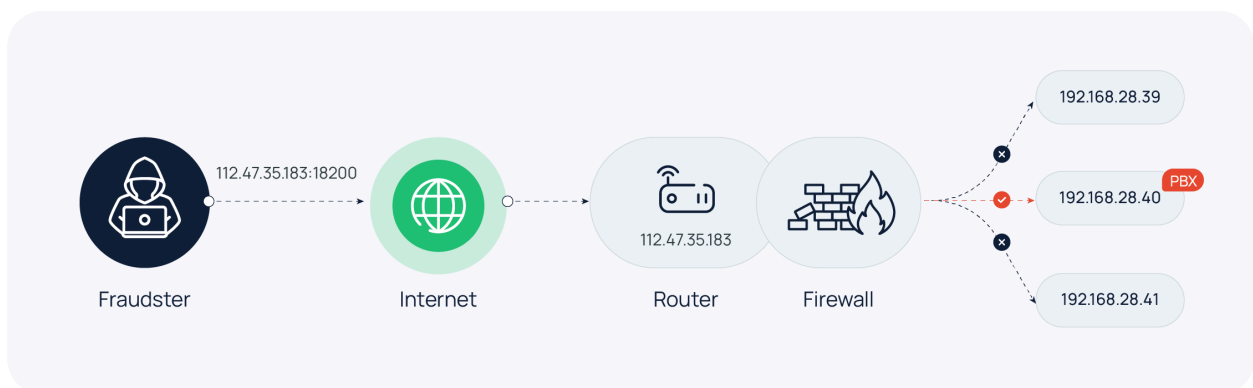
# Network Security

## Network Security

Network Security is the second line of defense in multi-layered security strategy, monitoring access to your phone system, accepting or denying access based on a set of pre-defined rules. You can enhance network security by utilizing **Remote Access Service, Global Anti-hacking IP Blocklist, Allowed Country IPs, Static Defense, and Auto Defense** policies.

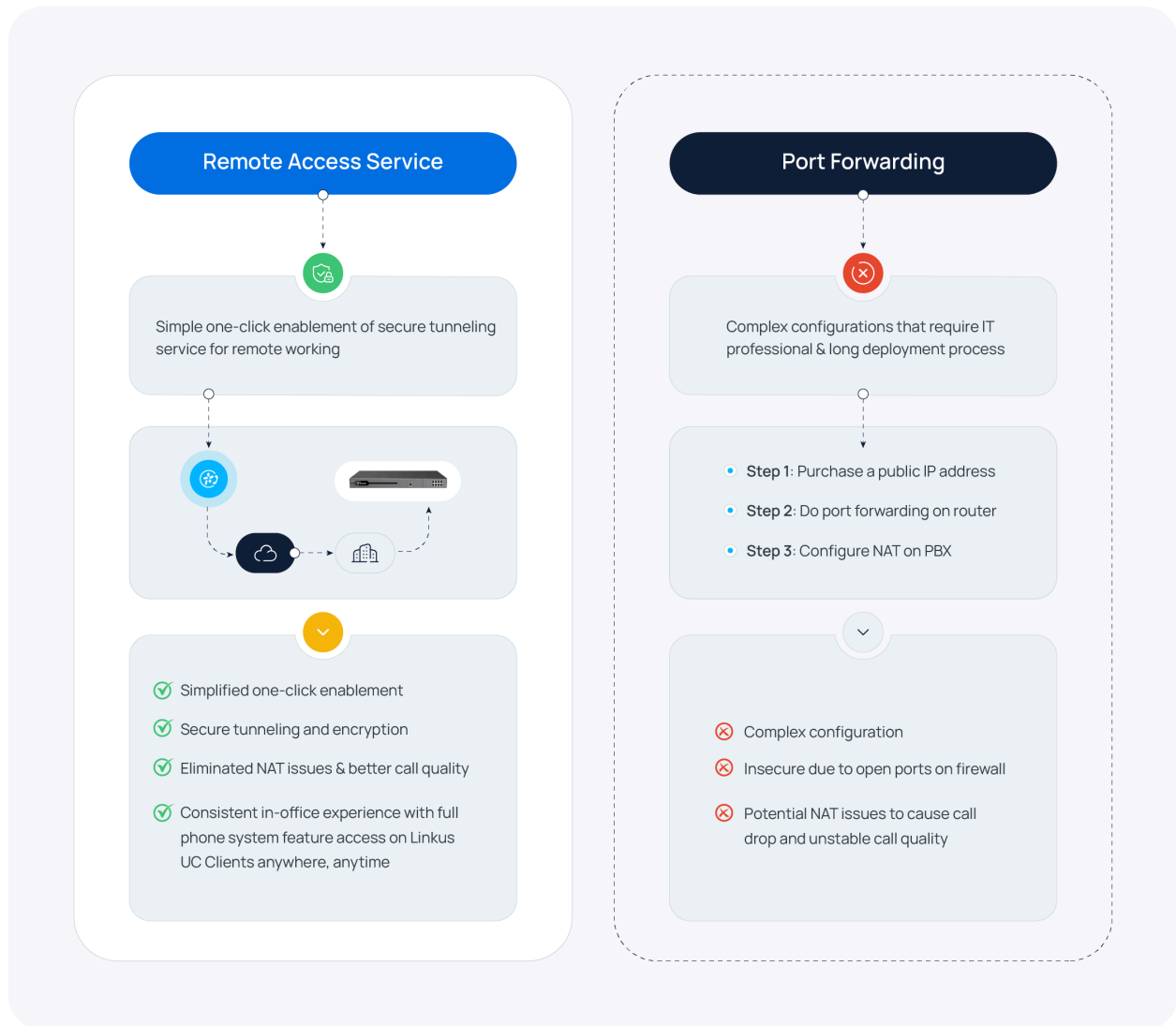
### Avoid Port Forwarding for Remote Access

In an attempt to offer remote access for remote and mobile users, most on-premises PBX providers will recommend Port Forwarding. Essentially, Port Forwarding maps an external port on your public IP address to the PBX that is within your Local Area Network (LAN). This exposes your PBX on the Internet and brings potential risks, because hackers could penetrate your network through the forwarded port.



Yeastar P-Series PBX System supports Remote Access Service (RAS), which allows for remote access without port forwarding. It provides an easy-to-access domain name for you to customize your PBX URL and allows you to perform daily business communications and administration with Linkus UC Clients anywhere. Moreover, RAS offers advanced access control to ensure further security. You can permit or block remote access for SIP registration, web, Linkus, LDAP, and API, customize remote access authorization by extension or department, and apply IP restriction to further secure all the remote access.



**Note:**

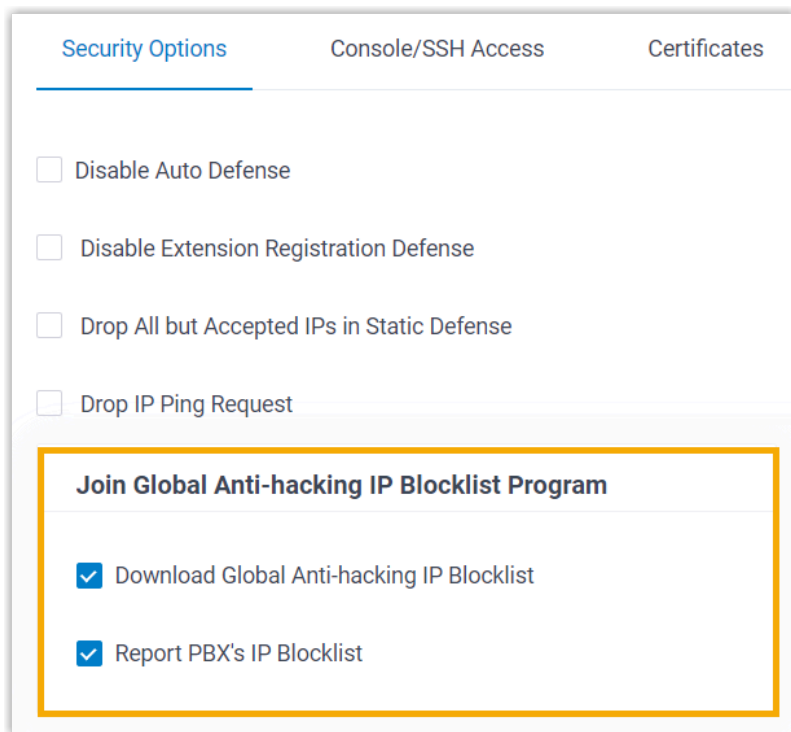
For more information about how to set up RAS, see [Yeastar Remote Access Service](#).

## Restrict Access to PBX by Yeastar-Shared IP Blocklist

Yeastar launches a **Global Anti-hacking IP Blocklist Program**, which centrally records a wide range of IP addresses that have been blocked by Yeastar PBXs worldwide and that are suspected of malicious activity or attack.

The IP blocklist is shared among all the Yeastar PBXs. With the Yeastar Global Anti-hacking IP Blocklist, all connections to your PBX from the IP addresses in the blocklist will be dropped, thus reducing the risk of cyber attacks.

Go to **Security > Security Settings > Security Options > Join Global Anti-hacking IP Blocklist Program** to double check that you have participated in the program.



## Restrict Access to PBX by Country/Region

Implement geographic restrictions to limit access to Yeastar P-Series PBX System from specific countries or regions. PBX will only allow access from your trusted geographic locations while blocking all other traffic.

To set up geographic restrictions, follow the instructions below:

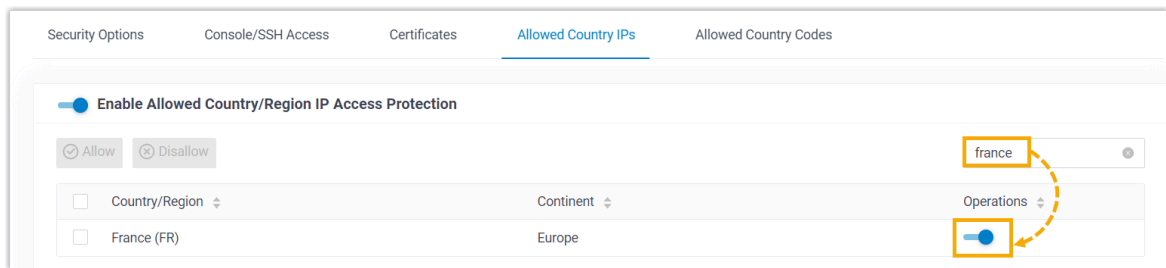
1. Go to **Security > Security Settings > Allowed Country IPs**.
2. Turn on the switch of **Enable Allowed Country/Region IP Access Protection**.



### Important:

If a pop-up appears, you **MUST** confirm to allow access from your country or region, or you will **NOT** be able to access your system.

3. At the top-right search bar, search the country or region that you want to grant access, then turn on the switch in the **Operations** column.



4. Click **Apply**.

## Restrict Access to PBX by Static Firewall Rules

Static Firewall Rules can monitor and control incoming traffic based on IP address, domain name, or MAC address, effective in protecting trusted connections and blocking known threats. There are default rules to accept access from your LAN, auto-provisioned devices, and Yeastar services. You can also add custom rules to **Accept**, **Drop**, or **Reject** specific traffic.

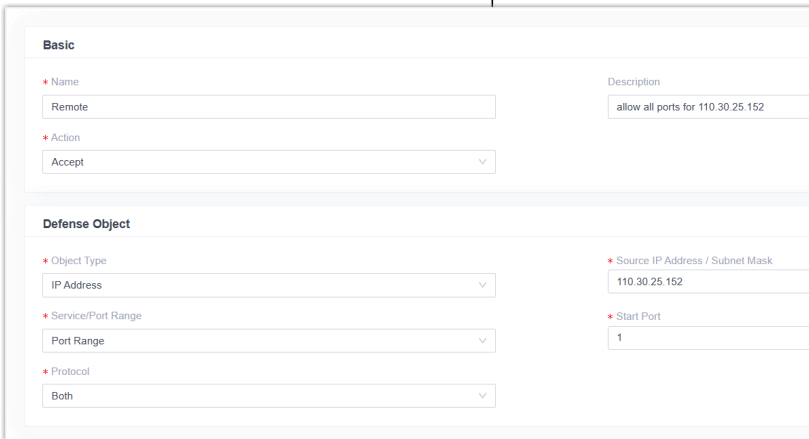
Go to **Security > Security Rules > Static Defense** to check the default rules and add custom rules as needed.

### Default Static Defense Rules

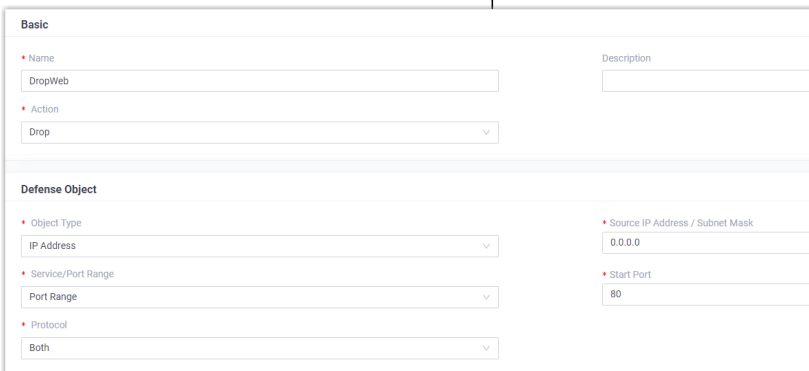
Static Defense						
Auto Defense    Blocked IPs    Outbound Call Frequency Restriction						
<div> <span>⊕ Add</span> <span>⊞ Import</span> <span>⊞ Export</span> <span>🗑 Delete</span> </div> <div> <span>All</span> <input type="text" value="Search"/> </div>						
<input type="checkbox"/>	Name	Defense Object	Action	Protocol	Service/Port Range	Operations
<input type="checkbox"/>	Default_Private_IPv4_1	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Default_Private_IPv4_2	172.16.0.0/16	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Default_Private_IPv4_3	10.0.0.0/8	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Default_Link-Local_IPv4_1	169.254.0.0/16	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Firmware Detection Server	255.255.255.255	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Remote Management Server_1	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Remote Management Server_2	172.16.0.0/16	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Remote Access Service	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Application Server	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	SMTP Server	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Activation Server	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Hot_Standby_Peer	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Hot_Standby_Virtual	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Automatically add 192.168.28.15	192.168.28.15	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Auto Provisioning Device	192.168.0.0/24	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Auto Provisioning Device	172.16.0.0/16	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>
<input type="checkbox"/>	Auto Provisioning Device	10.0.0.0/8	Accept	Both		<a href="#">🔗</a> <a href="#">🗑</a>

## Examples of Custom Static Defense Rule

**Table 1. Example 1: Accept remote registration from a trusted IP address**

Scenario	Setting
<p>Add a static defense rule to allow remote registration to Yeastar PBX.</p> <p>For example, the trusted IP address is 110.30.25.152.</p>	 <p>The screenshot shows the configuration for a static defense rule named 'Remote'. The action is set to 'Accept'. Under the 'Defense Object' section, the object type is 'IP Address', the source IP address/subnet mask is '110.30.25.152', the service/port range is 'Port Range', and the protocol is 'Both'. The description is 'allow all ports for 110.30.25.152'.</p>

**Table 2. Example 2: Block untrusted IP addresses from accessing PBX using HTTP with port 80**

Scenario	Setting
<p>Add a static defense rule to block web access from untrusted source.</p> <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #f0e68c;"> <p><b>! Important:</b></p> <ul style="list-style-type: none"> <li>Before you add the defense rule, ensure that there are rules to accept traffic from your LAN. Otherwise, you will NOT be able to access your phone system.</li> <li>Many attacks on PBX originate from web connection. We recommend that you set the restriction to protect against potential attacks.</li> </ul> </div>	 <p>The screenshot shows the configuration for a static defense rule named 'DropWeb'. The action is set to 'Drop'. Under the 'Defense Object' section, the object type is 'IP Address', the source IP address/subnet mask is '0.0.0.0', the service/port range is 'Port Range', and the protocol is 'Both'. The description is empty.</p>

## Restrict Access to PBX by Dynamic Firewall Rules

Dynamic Firewall Rules can block unknown threats by monitoring the packets sent within a specific time interval, effective in preventing massive connection attempts or brute force attacks. Yeastar P-Series PBX System has default auto defense rules to protect security of SSH connection, SIP registration, and web access. You can also add custom rules to strengthen the security.

### Default Auto Defense rules

Static Defense						
Auto Defense						
Blocked IPs						
Outbound Call Frequency Restriction						
<div><div><div><div></div></div><div>Add</div></div><div><div><div></div></div><div>Import</div></div><div><div><div></div></div><div>Export</div></div><div><div><div></div></div><div>Delete</div></div></div>						
<input type="checkbox"/>	Name	Service/Port Range	Port	Protocol	Rate	Operations
<input type="checkbox"/>	ssh	Service		TCP	10/60 s	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	udp	Service		UDP	40/2 s	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	tcp	Service		TCP	40/2 s	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	http	Service		Both	120/60 s	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/>	https	Service		Both	120/60 s	<a href="#">Edit</a> <a href="#">Delete</a>

### Example of Custom Auto Defense Rule

Table 3. Example: Block connections to Linkus

Scenario	Setting
Add a rule to block connections to Linkus if an IP address sends more than 120 packets in 60 seconds.	<div><div><div>Basic</div><div><div><div>* Name</div><div>Block_Connection_Linkus</div></div></div></div><div><div>Defense Object</div><div><div><div>* Service/Port Range</div><div>Service</div></div><div><div>* Protocol</div><div>Both</div></div><div><div>* Time Interval (s)</div><div>60</div></div><div><div>* Service</div><div>Linkus</div></div><div><div>* Number of IP Packets</div><div>120</div></div></div></div></div>

# Endpoint Security

## Extension Registration Security

Endpoint Security is the third line of defense in multi-layered security strategy, preventing fraudsters from registering or logging in to extension accounts. Yeastar P-Series PBX System has default rules to prevent malicious registration of SIP extensions by monitoring **Registration Attempts**, you can also enhance extension registration security by restricting **Registration Credential**, **Concurrent Registration**, **User Agent**, **IP Address**, and **Remote Registration**.

### Account Lockout for Failed Registration Attempts

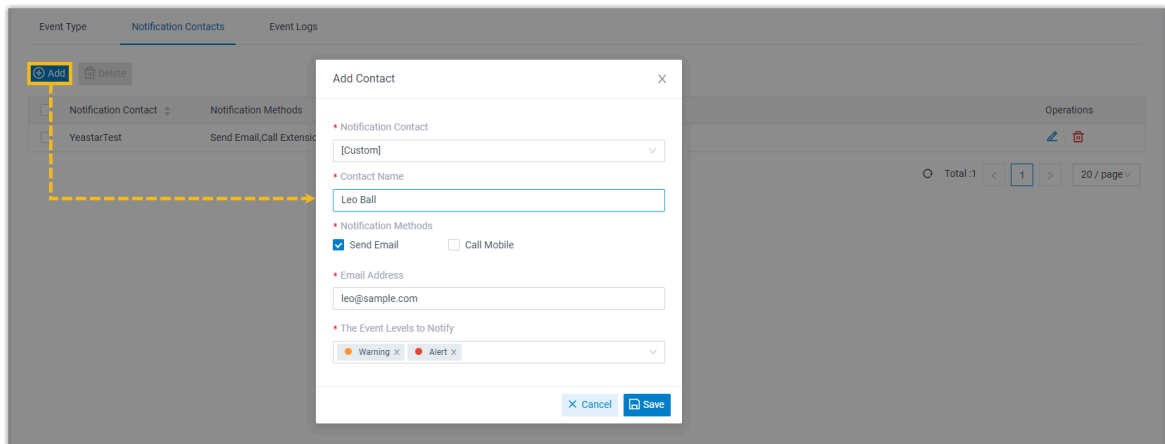
Yeastar P-Series PBX System has a built-in account lockout policy to prevent unauthorized access to extension accounts. It automatically locks the risky accounts after a certain number of failed registration attempts from the same IP address. When an account is locked, the PBX will block the source IP address, display it in **Blocked IPs**, and send an **Extension Registration Blocked Out** notification to the specified contacts.

To ensure that you can be notified when an account is locked out, you need to enable the event notification and add contacts to receive notifications.

1. Go to **System > Event Notification**.
2. Under **Event Type** tab, turn on the notification of **Extension Registration Blocked Out**.

Security			
Event Name	Event Level	Notification	Email Template
Web User Blocked Out	● Alert	<input checked="" type="checkbox"/>	<a href="#">✎</a>
Linkus User Blocked Out	● Alert	<input checked="" type="checkbox"/>	<a href="#">✎</a>
Extension Registration Blocked Out	● Alert	<input checked="" type="checkbox"/>	<a href="#">✎</a>

3. Under **Notification Contacts** tab, add contacts to receive event notifications.



After receiving notifications, you can check the details on PBX web portal (Path: **Security > Security Rules > Blocked IPs**).

Static Defense

Auto Defense

Blocked IPs

Outbound Call Frequency Restriction

🗑️ Delete

<input type="checkbox"/>	Defense Type ⌵	Block Type ⌵	Block Range ⌵	Time of Attack ⌵	Protocol ⌵	Attacked Port ⌵	Source IP	Operations
<input type="checkbox"/>	Extension Registration	Block Account	SIP Extension:1001	10/30/2023 02:32:28	SIP	SIP	110.87.9	🗑️

## Use Complex Credentials for SIP Registration

Weak SIP credentials leave a potential security gap that fraudsters can readily exploit. You can mitigate the risk by enforcing system-wide password length requirements and configuring strong registration credentials for all extensions.

### Enforce minimum registration password length

1. Go to **Security > Security Settings > Security Options**.
2. In the **Extension Password Rules** section, specify the minimum character length of registration password.

**Extension Password Rules**

\* Minimum Character Length of User Password

10

\* Minimum Character Length of Registration Password

8

☐ Extensions Are Not Allowed Reuse Any of Their Last

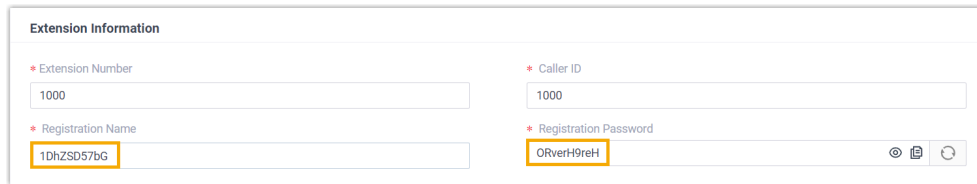
3

User Password(s)

3. Click **Save** and **Apply**.

### Configure strong registration credentials for extension

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **Extension Information** section, set complex registration name and registration password.



The screenshot shows the 'Extension Information' form. It has four main fields: 'Extension Number' (1000), 'Caller ID' (1000), 'Registration Name' (10hzSD57bG), and 'Registration Password' (ORverH9reH). The 'Registration Name' and 'Registration Password' fields are highlighted with yellow boxes. There are also icons for copy, paste, and refresh on the right side of the password field.

**Tip:**

Here are some tips for a complex credential:

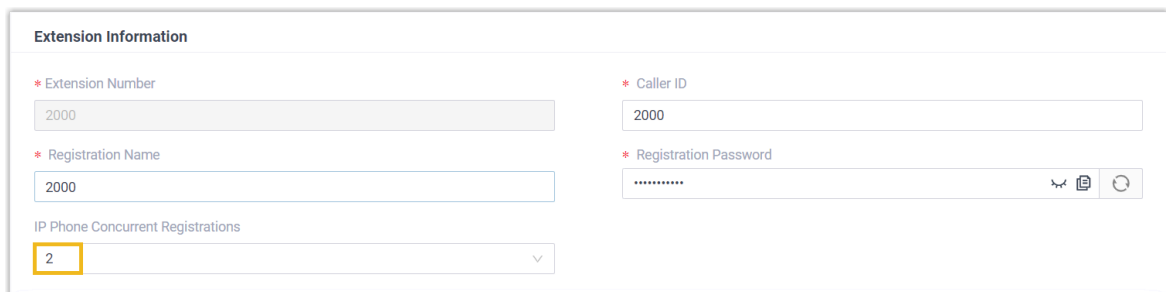
- Use a combination of uppercase letters, lowercase letters, and numbers.
- Avoid repeated or consecutive numbers.
- Avoid extension number or extension name.

3. Click **Save** and **Apply**.

## Restrict Multiple Registrations on the Same Extension

By default, Yeastar P-Series PBX System allows one extension to be registered on a single device only. We recommend that you keep the restriction UNLESS you need multiple devices to register with a single SIP extension. If necessary, you can increase the concurrent registration limit for a SIP extension as follows:

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **Extension Information** section, select a value from the drop-down list of **IP Phone Concurrent Registrations**.



The screenshot shows the 'Extension Information' form. It has four main fields: 'Extension Number' (2000), 'Caller ID' (2000), 'Registration Name' (2000), and 'Registration Password' (masked with dots). The 'IP Phone Concurrent Registrations' dropdown menu is highlighted with a yellow box and shows the value '2'. There are also icons for copy, paste, and refresh on the right side of the password field.

3. Click **Save** and **Apply**.

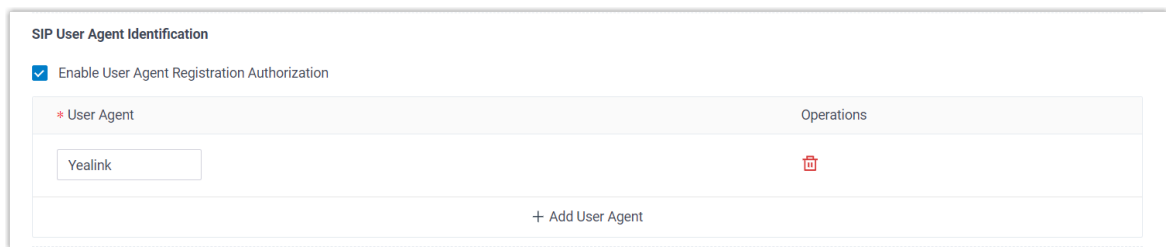


## Restrict Extension Registration by User Agent

Restrict extension registration by authenticating user agent. When registering, SIP phones will send packets containing a user agent string. If the prefix of the user agent does not match the defined value, the registration will fail.

To restrict extension registration by user agent, follow the instructions below:

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. Under **Security** tab, select the checkbox of **Enable User Agent Registration Authorization**, and set up the user agent.



The screenshot shows the 'SIP User Agent Identification' configuration window. At the top, there is a checkbox labeled 'Enable User Agent Registration Authorization' which is checked. Below this is a table with two columns: '\* User Agent' and 'Operations'. The table contains one row with the value 'Yealink' in the first column and a trash icon in the second column. At the bottom of the table, there is a '+ Add User Agent' button.

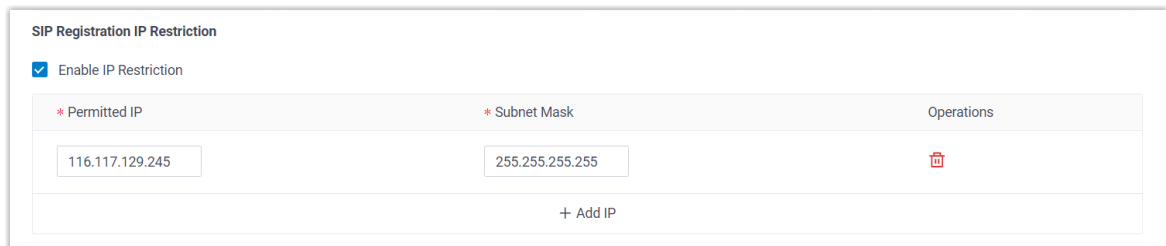
3. Click **Save** and **Apply**.

## Restrict Extension Registration by IP Address

Restrict extension registration to trusted IP addresses. In this way, the system will automatically drop registration requests from untrusted IPs to prevent unauthorized devices from registering.

To restrict extension registration by IP address, follow the instructions below:

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. Under **Security** tab, select the checkbox of **Enable IP Restriction** and add the allowed IP address.



The screenshot shows the 'SIP Registration IP Restriction' configuration window. At the top, there is a checkbox labeled 'Enable IP Restriction' which is checked. Below this is a table with three columns: '\* Permitted IP', '\* Subnet Mask', and 'Operations'. The table contains one row with the value '116.117.129.245' in the first column, '255.255.255.255' in the second column, and a trash icon in the third column. At the bottom of the table, there is a '+ Add IP' button.

3. Click **Save** and **Apply**.

## Restrict Remote Registration

If remote SIP access via Yeastar FQDN is enabled, we recommend that you implement account and IP restrictions to enhance the security of remote registration.

1. Go to **System > Network > Yeastar FQDN**.
2. In the **Features** section, click **SIP Access** tab.

**Features**

**SIP Access** Remote Access

Before enabling this feature, please make sure your extensions are using strong registration passwords, or it might bring security risks.

\* Status  
Enabled

Remote Access Service Port-SIP UDP&TCP

Remote Access Service Port-SIP TLS

3. Set restrictions for extension accounts.

**Access Type**

**a** Allowed Account

**Available** (21 items)

Extension Number	Caller ID Name
1007	1007
1008	1008
1009	1009
1010	Olivia Su
1011	wym_wangym_yeastar8...

**Selected** (4 items)

Extension Number	Caller ID Name
1001	Phillip Huff
1002	Terrell Smith
1003	Dave Harris
1004	Naomi Nichols

**b**

- a. In the **Access Type** drop-down list, select a type.
    - **Allowed Account:** Only the selected accounts can register remotely via Yeastar FQDN.
    - **Restricted Account:** All accounts except for the selected accounts can register remotely via Yeastar FQDN.
  - b. Select the desired accounts from the **Available** box to the **Selected** box.
4. Set restrictions for IP addresses.

- a. Select the checkbox of **Enable IP Restriction**.
  - b. Click **Add** to add the IP addresses that are allowed to register extensions remotely via Yeastar FQDN.
5. Click **Save** and **Apply**.

## Extension Login Security

Endpoint Security is the third line of defense in multi-layered security strategy, preventing fraudsters from registering or logging in to extension accounts. Yeastar P-Series PBX System has default rules to prevent malicious login to SIP extensions by monitoring **Login Attempts**, you can also enhance extension login security by utilizing the **Single Sign-on (SSO)**, **Two-factor Authentication (2FA)**, **Login QR Code/Link**, **Password**, **User Role**, **Account & IP** policies.

### Account Lockout for Failed Login Attempts

Yeastar P-Series PBX System has a built-in account lockout policy to prevent unauthorized access to PBX web portal and Linkus clients:

- If an IP address reaches the defined number of failed login attempts within a specific time period, the IP address will be denied further attempts temporarily.
- If the IP address reaches the maximum number of failed login attempts, the IP address will be banned from logging into the account permanently. The PBX will block the IP address, display it in **Blocked IPs**, and send notifications of **Web User Blocked Out** or **Linkus User Blocked Out** to the specified contacts.

To ensure that you can be notified when an IP address is blocked, you need to enable the event notification and add contacts to receive notifications.

1. Go to **System > Event Notification**.
2. Under **Event Type** tab, turn on the notification of **Web User Blocked Out** and **Linkus User Blocked Out**.

Event Type

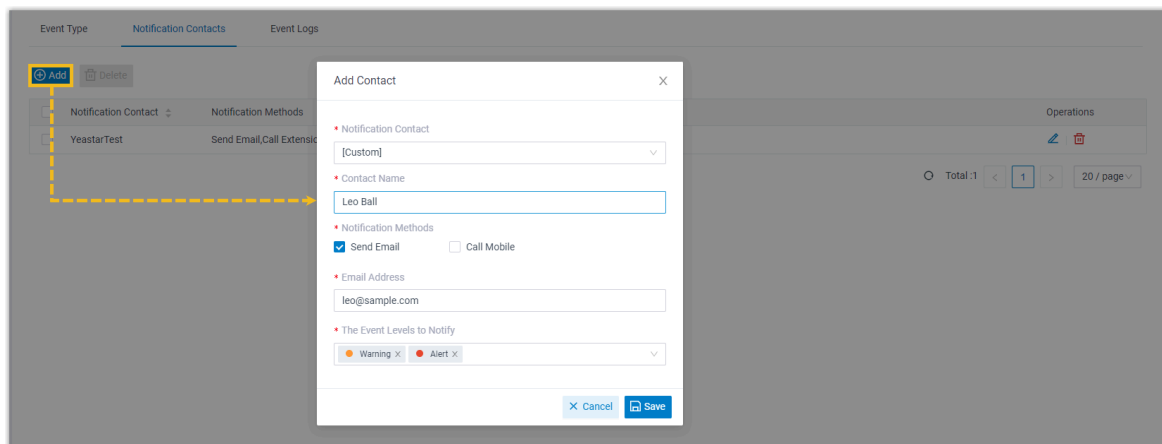
Notification Contacts

Event Logs

Security

Event Name	Event Level	Notification	Email Template
Web User Blocked Out	<div><div></div>Alert</div>	<div><div></div></div>	<div></div>
Linkus User Blocked Out	<div><div></div>Alert</div>	<div><div></div></div>	<div></div>

3. Under **Notification Contacts** tab, add contacts to receive event notifications.



After receiving notifications, you can check the details on PBX web portal (Path: **Security > Security Rules > Blocked IPs**).

Static Defense

Auto Defense

Blocked IPs

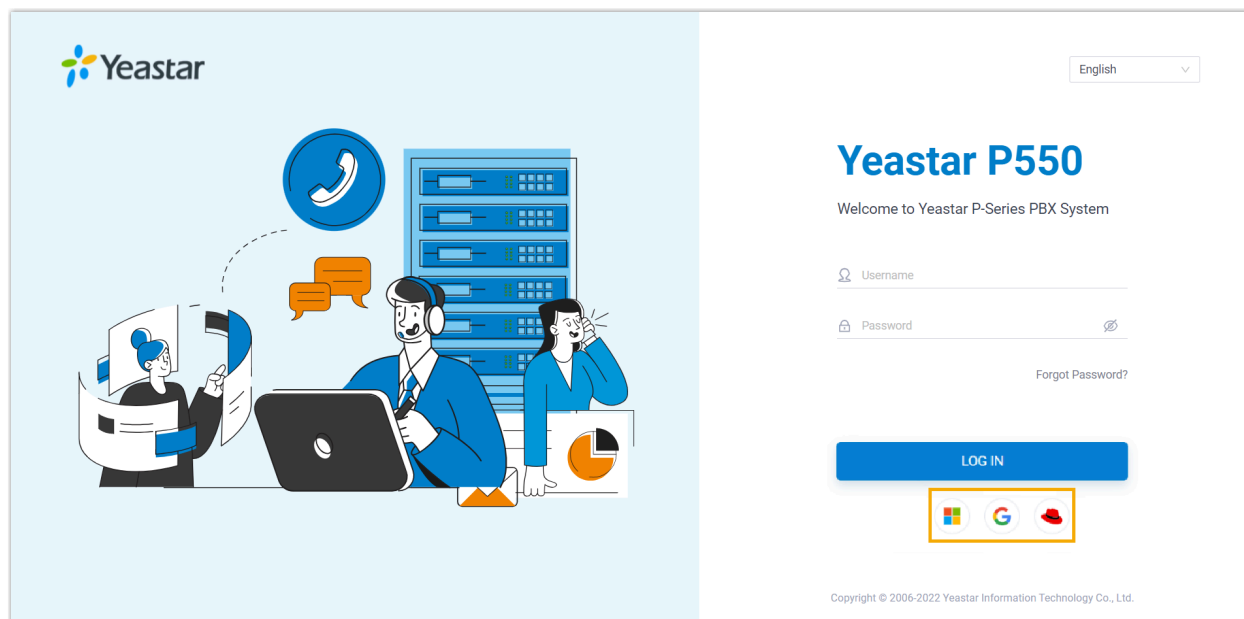
Outbound Call Frequency Restriction

Delete

<input type="checkbox"/>	Defense Type ▾	Block Type ▾	Block Range ▾	Time of Attack ▾	Protocol ▾	Attacked Port ▾	Source IP	Operations
<input type="checkbox"/>	Web Login	Block Account	WebUser:1000	10/30/2023 02:11:07	HTTPS	14500	110.87.9	<div></div>

## Single Sign-on (SSO) for Third-party Authentication

The integration between Yeastar P-Series PBX System and **Microsoft 365/Google Workspace/Red Hat SSO** supports Single Sign-on (SSO) feature, which allows users to log in to Linkus UC Clients using their Microsoft/Google/Red Hat accounts, eliminating the need to remember multiple credentials while enhancing security by leveraging the security policies of third-party accounts.



- To allow users to log in to Linkus UC Clients using their **Microsoft 365** accounts, you need to integrate the PBX with **Microsoft Entra ID (Azure Active Directory)** or **Active Directory**, and enable SSO.

For more information on how to set up the integration, see [Microsoft Entra ID Integration Guide](#) and [Active Directory Integration Guide](#).

- To allow users to log in to Linkus UC Clients using their **Google** accounts, you need to integrate the PBX with **Google Workspace**, and enable SSO.

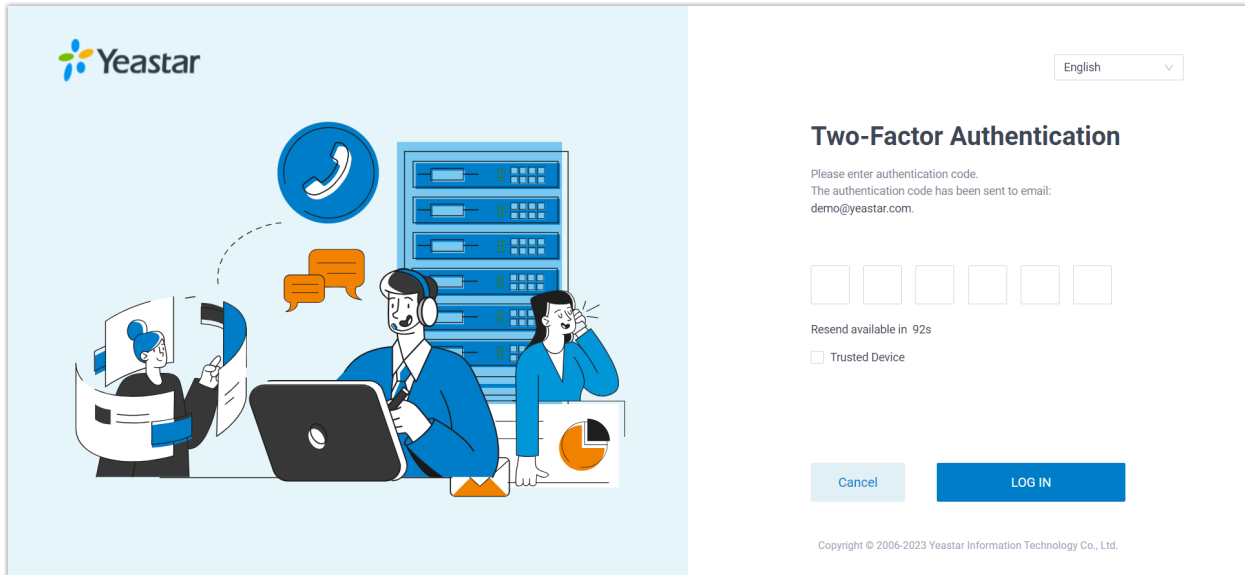
For more information on how to set up the integration, see [Google Workspace Integration Guide](#).

- To allow users to log in to Linkus UC Clients using their **Red Hat** accounts, you need to integrate the PBX with **Red Hat SSO**, and enable SSO.

For more information on how to set up the integration, see [Red Hat SSO Integration Guide](#).

## Two-factor Authentication (2FA) for Enhanced Login Security

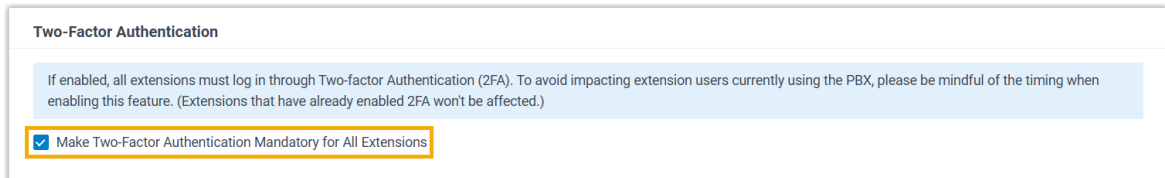
Two-factor Authentication (2FA) provides an extra layer of security to protect account by requiring two verification factors to log in. The first factor is the password that is used to log in to account, the second factor is a code that is sent to a specified device.



The image shows the Yeastar Two-Factor Authentication login interface. On the left, there is a blue illustration of three people working at a desk with a laptop and server racks in the background. The Yeastar logo is in the top left corner. In the top right, there is a language dropdown menu set to 'English'. The main heading is 'Two-Factor Authentication'. Below it, a message states: 'Please enter authentication code. The authentication code has been sent to email: demo@yeastar.com.' There are six empty square boxes for entering the code. Below the boxes, it says 'Resend available in 92s' and a checkbox for 'Trusted Device'. At the bottom, there are 'Cancel' and 'LOG IN' buttons. A copyright notice 'Copyright © 2006-2023 Yeastar Information Technology Co., Ltd.' is at the very bottom.

You can enforce 2FA for all extension users, ensuring that every user must provide both account password and an authentication code when logging in to their accounts.

1. Go to **Security > Security Settings > Security Options**.
2. In the **Two-Factor Authentication** section, select the checkbox of **Make Two-Factor Authentication Mandatory for All Extensions**.



The image shows the 'Two-Factor Authentication' settings panel. It has a title 'Two-Factor Authentication' and a descriptive text: 'If enabled, all extensions must log in through Two-factor Authentication (2FA). To avoid impacting extension users currently using the PBX, please be mindful of the timing when enabling this feature. (Extensions that have already enabled 2FA won't be affected.)' Below this text is a checkbox labeled 'Make Two-Factor Authentication Mandatory for All Extensions', which is checked and highlighted with an orange border.

3. Click **Save** and **Apply**.



**Note:**

If 2FA is not enforced, each extension user can choose to enable or skip 2FA for their account in Linkus Desktop or Web Client. For more information, see [Enable 2FA on Linkus Desktop Client](#) and [Enable 2FA on Linkus Web Client](#).

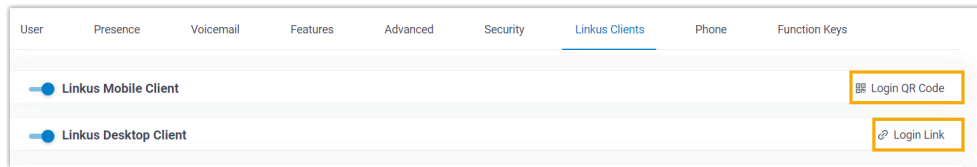
## QR Code/Link for Passwordless Login

QR Code Authentication and Link Authentication are more secure ways to log in to Linkus clients than traditional password login, as they are encrypted and can only be used ONCE.

You can send the Linkus login QR code/link to users in the following ways:

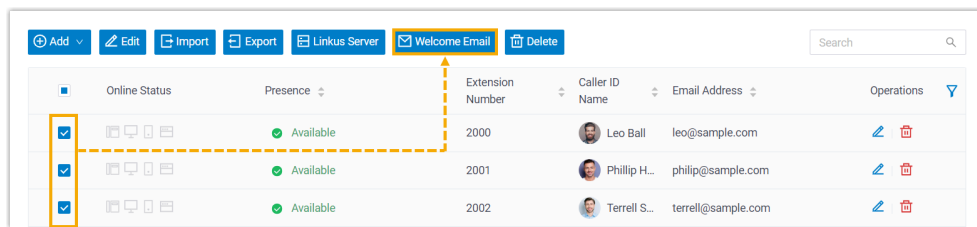
### Provide a single user with login QR code/link

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. Under **Linkus Clients** tab, click **Login QR Code** or **Login Link** to copy the credential and send to users.



## Provide multiple users with login QR code/link

1. Go to **Extension and Trunk > Extension**.
2. Select the desired extensions, then click **Welcome Email**.

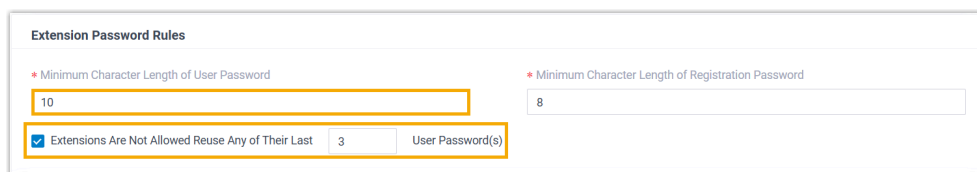


## Strong Password for Manual Login

Weak passwords leave a potential security gap that fraudsters can readily exploit. You can mitigate the risk by enforcing system-wide password requirements and configuring strong passwords for extensions.

### Enforce password policies

1. Go to **Security > Security Settings > Security Options**.
2. In the **Extension Password Rules** section, specify the minimum character length of user password, and the number of recently used passwords that cannot be reused.



3. Click **Save** and **Apply**.

## Configure strong password for extension

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **User Information** section, set a strong user password.

The screenshot shows the 'User Information' form. It has two columns. The left column contains 'First Name' (with '1000' entered), 'Email Address', and 'User Password' (with '10hZSD57bG' entered and highlighted by a yellow box). The right column contains 'Last Name', 'Mobile Number', and 'User Role' (set to 'None').



### Tip:

Here are some tips for a strong password:

- Use a combination of uppercase letters, lowercase letters, and numbers.
- Avoid repeated or consecutive numbers.
- Avoid extension number or extension name.

3. Click **Save** and **Apply**.

## User Role for Granular Access Control

Role-based access control is a security approach that authorizes or restricts system access permissions to users based on their roles within the company. This allows users to access the administrative privileges they need to conduct their jobs, and minimizes the risk of unauthorized users accessing sensitive information or performing unauthorized tasks.

Yeastar P-Series PBX System has built-in roles: **Super Administrator**, **Administrator**, **Supervisor**, **Operator**, **Employee**, **Human Resource**, **Accounting**, and **Hotel Manager**.

You can use the built-in roles and assign them to employees without further configuration, or create your own custom roles with the exact set of permissions you need.

### Create a Custom Role

1. Go to **Extension and Trunk > Role**.
2. Click **Add** to create a role from scratch, or click **Copy Role** to create a role by copying an existing role.





## Assign Roles to Users

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **User Information** section, select a role from the drop-down list of **User Role**.

**User Information**

First Name: Terrell Smith

Last Name:

Email Address: terrell@sample.com

Mobile Number: 15880123456

\* User Password:





User Role: Administrator

3. Click **Save** and **Apply**.

## Account and IP restrictions for Remote Login

If remote access to Linkus UC Clients via Yeastar FQDN is enabled, we recommend that you implement account and IP restrictions to enhance the security of remote login.

1. Go to **System > Network > Yeastar FQDN**.
2. In the **Features** section, click **Remote Access** tab, then edit web access or Linkus access as needed.

Features						
SIP Access	Remote Access					
Name	Status	Remote Access Service Port	Permitted IP	Access Type	Number of Account	Operations
Web Access	Enabled	8080	All	Restricted	1	
Linkus Access	Enabled	8080	All	--	--	
LDAP Access	Disabled	--	All	--	--	
API Access	Disabled	--	All	--	--	

### 3. Set restrictions for extension accounts.

Edit

Name

Web Access

\* Status

Enabled

Remote Access Service Port

8080

Access Type

Allowed Account

Select Account

1001-Phillip Huff ×

1002-Terrell Smith ×

1003-Dave Harris ×

1004-Naomi Nichols ×

☐ Enable IP Restriction

× Cancel

✓ Confirm

a. In the **Access Type** drop-down list, select a type.

- **Allowed Account:** Only the selected accounts can remotely log in to Linkus Web Client via Yeastar FQDN.
- **Restricted Account:** All accounts except for the selected accounts can remotely log in to Linkus Web Client via Yeastar FQDN.

b. In the **Select Account** drop-down list, select the desired accounts.

### 4. Set restrictions for IP addresses.

The screenshot shows a web interface for configuring IP restrictions. At the top, there is a checkbox labeled 'Enable IP Restriction' which is checked. Below this, there is a table with two columns: 'Permitted IP' and 'Subnet Mask'. The first row contains the IP address '110.77.35.10' and the subnet mask '255.255.255.0'. To the right of the table, there is an 'Operations' column with a trash icon. Below the table, there is a '+ Add' button. A yellow box labeled 'a' highlights the 'Enable IP Restriction' checkbox, and a yellow box labeled 'b' highlights the '110.77.35.10' IP address.

Permitted IP	Subnet Mask	Operations
110.77.35.10	255.255.255.0	

[+ Add](#)

- a. Select the checkbox of **Enable IP Restriction**.
  - b. Click **Add** to add the IP addresses that are allowed to remotely log in to Linkus UC Clients via Yeastar FQDN.
5. Click **Confirm**.
  6. Click **Save** and **Apply**.

# Outbound Call Security

## Outbound Call Security

Outbound Call Security is the last line of defense in multi-layered security strategy, restricting outbound calls from Yeastar P-Series PBX System based on a set of pre-defined rules and minimizing the losses caused by toll fraud if there is any. You can enhance outbound call security by restricting **Outbound Route Permission, PIN Code, Time Condition, Country/Region, Phone Number, Call Frequency, Concurrent Calls, and Call Duration.**

### Restrict Outbound Dialing by Outbound Route Permission

Employees perform different tasks in a company, and not all of them need to make outbound calls. When configuring the PBX for outbound dialing, consider setting different outbound routes for different trunks (e.g. local, long-distance, international, etc.), and assign outbound route permission only to the extension users that require the use of it.

<input type="checkbox"/>	Name	Outbound Caller ID	Dial Pattern	Trunk	Extension/Group	Move	Operations
<input type="checkbox"/>	Local_Calls		8X.	Local	Extension Group...	↑   ↓	✎   🗑
<input type="checkbox"/>	Long_Dist...		0X.	Long_Dist...	Extension Group...	↑   ↓	✎   🗑
<input type="checkbox"/>	Internatio...		9X.	Internati...	2000-Leo Ball 2001-Phillip Hu...	↑   ↓	✎   🗑

### Restrict Outbound Dialing by PIN Code

Set password for outbound route to require callers to enter a PIN code before dialing out. Only when a valid PIN code is entered can the call be routed out through the outbound route.

You can set a single PIN or multiple PINs for an outbound route.

#### Set a single PIN for an outbound route

1. Go to **Call Control > Outbound Route**, edit the desired outbound route.

2. In the **Outbound Route Password** drop-down list, select **Single PIN** and set a PIN code.

3. Click **Save** and **Apply**.

## Set multiple PINs for an outbound route

1. Create a PIN list on **Call Features > PIN List**.

2. Associate the PIN list with outbound route on **Call Control > Outbound Route > Outbound Route Password**.

3. Click **Save** and **Apply**.

## Restrict Outbound Dialing by Time Condition

Hacking attempts are usually made during non-business hours, over weekends, and during holiday periods when the system is less attended. You can configure different outbound call restriction rules for different time periods to reinforce security. For example, you might create a Time Condition called “Business Hours”, and only allow outbound calls during business hours by applying the Time Condition to an outbound route, as shown below.

## 1. Create a Time Condition on **Call Control > Business Hours and Holidays**.

## 2. Apply the Time Condition to an outbound route.

a. Go to **Call Control > Outbound Route**.

b. In the **Time Condition** section, select a time condition to limit when outbound calls can be made using the outbound route.

c. Click **Save** and **Apply**.



### Note:

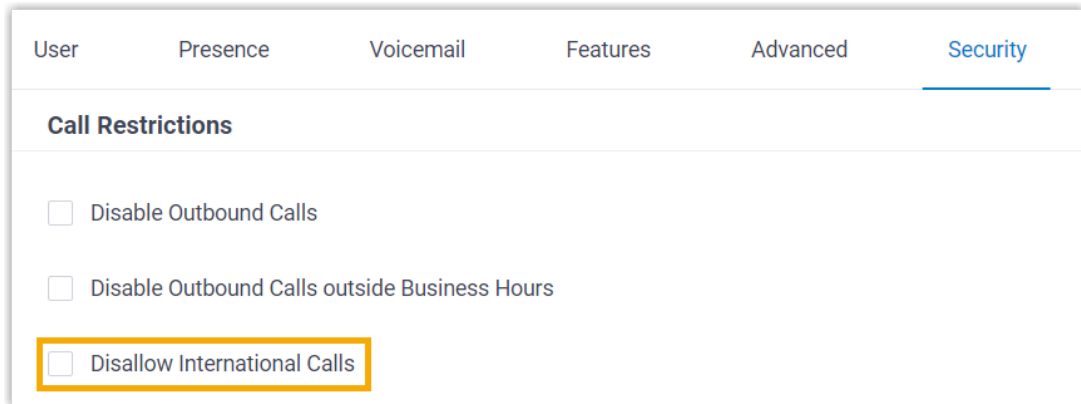
For detailed introduction and instruction about **Time Condition**, see [Overview of Business Hours and Holidays](#).

## Restrict Outbound Dialing by Country/Region

If your company is engaged in international business and your employees need to interact with partners or customers over the phone, you can set up international dialing on the PBX. However, this puts your system in the danger of international toll fraud and may result in significant financial loss.

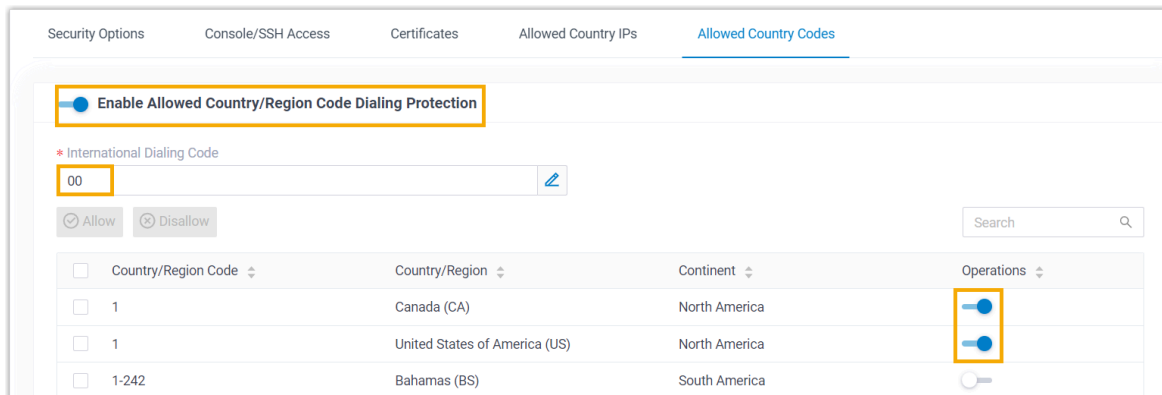
To mitigate the risk, we recommend that you restrict the international dialing permission only to the extension users and countries /regions that are required.

1. Grant international dialing permission to the desired extension user.
  - a. Go to **Extension and Trunk > Extension**, edit the desired extension.
  - b. Under **Security** tab, unselect the checkbox of **Disallow International Calls**.



The screenshot shows the 'Security' tab of an extension configuration page. Under the 'Call Restrictions' section, there are three checkboxes: 'Disable Outbound Calls', 'Disable Outbound Calls outside Business Hours', and 'Disallow International Calls'. The 'Disallow International Calls' checkbox is highlighted with a yellow rectangular box.

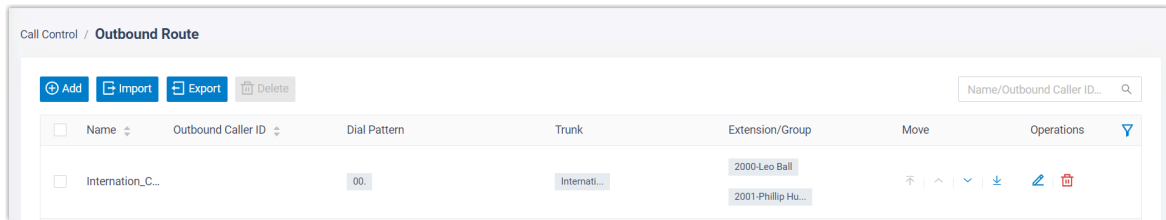
- c. Click **Save** and **Apply**.
2. Enable international dialing to the desired countries or regions.



The screenshot shows the 'Allowed Country Codes' configuration page. At the top, the 'Enable Allowed Country/Region Code Dialing Protection' switch is turned on and highlighted with a yellow box. Below it, the 'International Dialing Code' field contains '00'. There are 'Allow' and 'Disallow' buttons. A table lists countries/regions with their codes, names, continents, and operation status. The 'Operations' column has switches for each entry: Canada (CA), United States of America (US), and Bahamas (BS). The switches for Canada and the US are turned on and highlighted with yellow boxes.

Country/Region Code	Country/Region	Continent	Operations
1	Canada (CA)	North America	On
1	United States of America (US)	North America	On
1-242	Bahamas (BS)	South America	Off

- a. Go to **Security > Security Settings > Allowed Country Codes**.
  - b. Turn on the switch of **Enable Allowed Country/Region Code Dialing Protection**.
  - c. In the **International Dialing Code** field, enter the dialing prefix of international call for your country.
  - d. In the **Operations** column, enable the desired country or region.
  - e. Click **Apply**.
3. Ensure that there is at least one outbound route that matches the international dialing code and is available for the extension user to dial out.



## Restrict Outbound Dialing by Phone Number

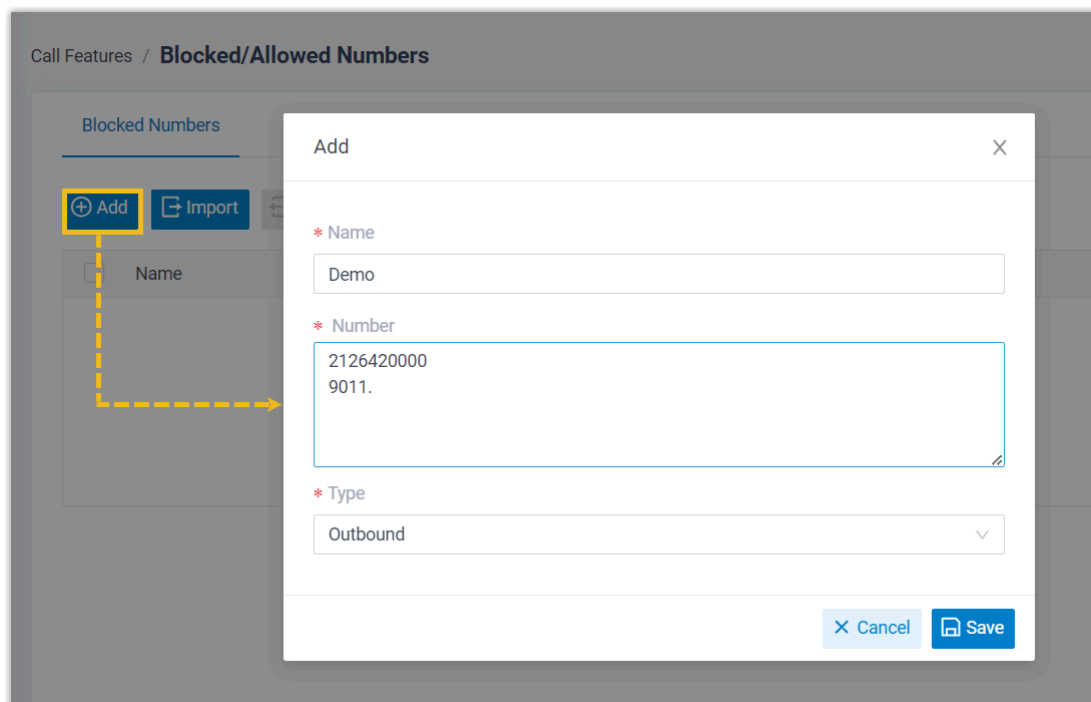
Toll fraud happens when someone gains access to your phone system and generates a high volume of calls to premium rate numbers. As a result, fraudsters take revenues generated from these calls, while you get a costly telephone bill. It is advisable to restrict outbound calls to such premium rate numbers. This can be achieved by blocking specific phone numbers or number patterns.

1. Go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. Click **Add** to add the phone numbers that users can not dial out.



### Tip:

You can enter specific numbers or number patterns. For detailed introduction about number pattern, see [Number Pattern](#).





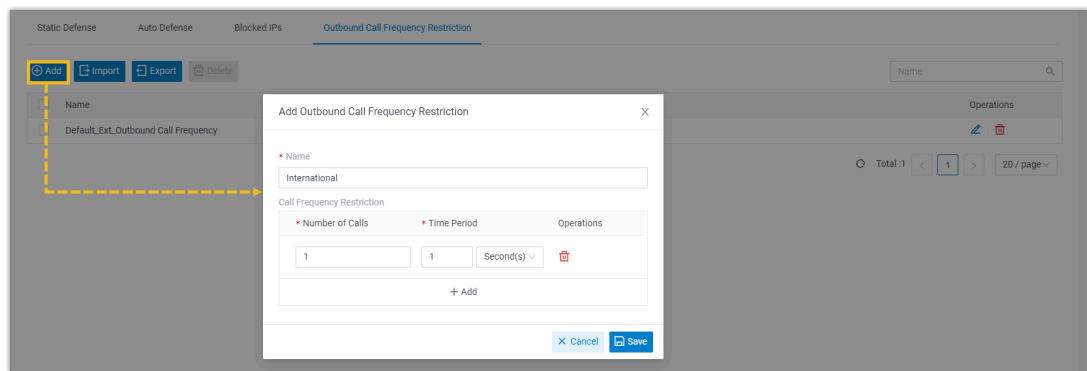
3. Click **Save** and **Apply**.

## Restrict Outbound Dialing by Frequency of Calls

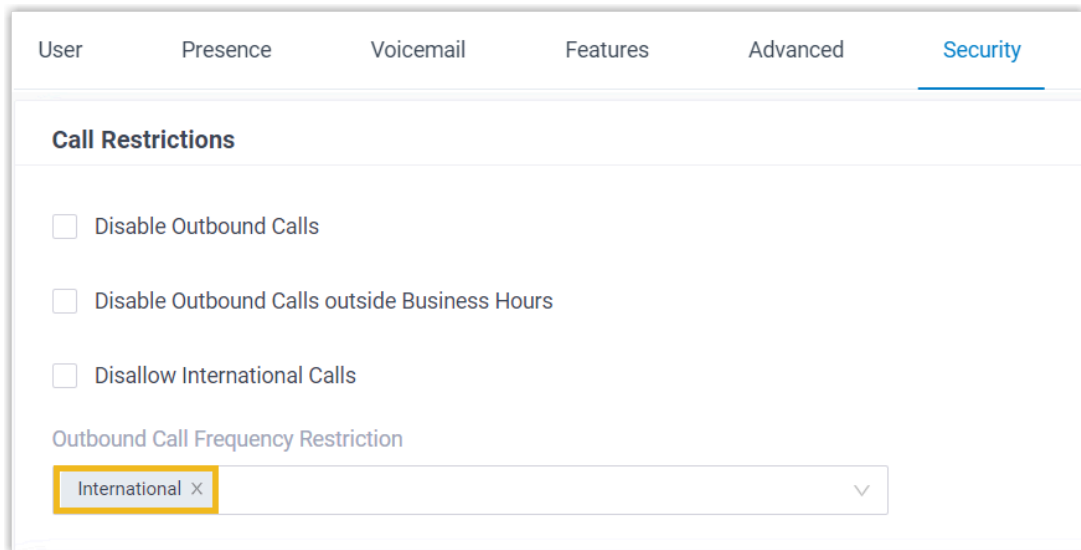
Limit the number of outbound calls that extension users can make within a certain time period. When the limit is reached, any further outbound calls from the extension will be denied.

Yeastar P-Series PBX System has a default rule, restricting that each extension user can make up to 5 outbound calls per second. You can use the default rule, or customize a rule and associate it with the desired extension users.

1. Create a custom restriction rule.
  - a. Go to **Security > Security Rules > Outbound Call Frequency Restriction**.
  - b. Click **Add** to add a rule.



- c. Click **Save**.
2. Associate the custom rule with desired extension users.
  - a. Go to **Extension and Trunk > Extension**, edit the desired extension.
  - b. Under **Security** tab, select the custom rule from the drop-down list of **Outbound Call Frequency Restriction**.



User   Presence   Voicemail   Features   Advanced   **Security**

**Call Restrictions**

☐ Disable Outbound Calls

☐ Disable Outbound Calls outside Business Hours

☐ Disallow International Calls

Outbound Call Frequency Restriction

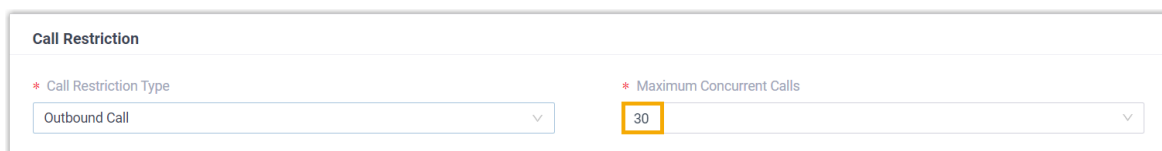
International ×

c. Click **Save** and **Apply**.

## Restrict Outbound Calling by Concurrent Calls

Limit the number of simultaneous outbound calls on SIP trunks, so as to prevent fraudsters from generating a high volume of calls over the trunks without limitation.

1. Go to **Extension and Trunk > Trunk**, edit the desired SIP trunk.
2. Under **Advanced** tab, select or enter a value in the **Maximum Concurrent Calls** field.



Call Restriction

\* Call Restriction Type

Outbound Call

\* Maximum Concurrent Calls

30

3. Click **Save** and **Apply**.

## Restrict Outbound Calling by Call Duration

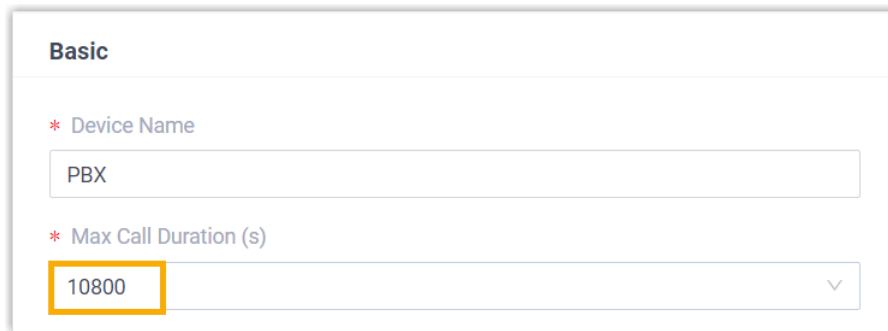
Set restrictions on the duration of outbound calls to automatically end calls when reaching the specified time limit, this will help you prevent potential misuse of the phone system and control call costs.

You can implement call duration control on a global basis or on a per-user basis.

### Limit Outbound Call Duration for All Users (Global Setting)

1. Go to **PBX Settings > Preferences**.

2. In the **Basic** section, select or enter a value in the **Max Call Duration (s)** field.

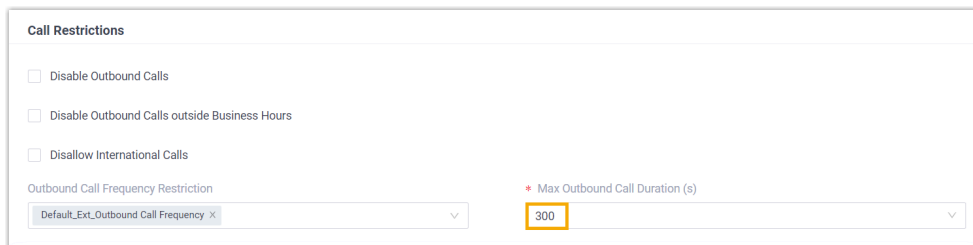


The screenshot shows a configuration window titled "Basic". It contains two fields: "Device Name" with the value "PBX" and "Max Call Duration (s)" with the value "10800". The "Max Call Duration (s)" field is highlighted with a yellow border.

3. Click **Save** and **Apply**.

### Limit Outbound Call Duration for Specific Users (Per-User Setting)

1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. Under **Security** tab, select a value from the drop-down list of **Max Outbound Call Duration (s)**.



The screenshot shows a configuration window titled "Call Restrictions". It contains three checkboxes: "Disable Outbound Calls", "Disable Outbound Calls outside Business Hours", and "Disallow International Calls". Below these is a section for "Outbound Call Frequency Restriction" with a dropdown menu showing "Default\_Ext\_Outbound Call Frequency X". To the right is a field for "Max Outbound Call Duration (s)" with the value "300". The "Max Outbound Call Duration (s)" field is highlighted with a yellow border.

3. Click **Save** and **Apply**.

# Contingency Plan

## Contingency Plan

Although anti-hacking measures can be taken to protect your phone system, there is no absolute safety. Therefore, a contingency plan should be in place to ensure a timely and effective response in case fraudsters successfully infiltrate your PBX or force your PBX to fail. You can utilize the **Event Notification and Logging** policy to monitor and get notified of critical events in real time, and the **Backup and Archive** policy to back up data and configurations in case of system failure or data loss.

### Event Notification and Logging

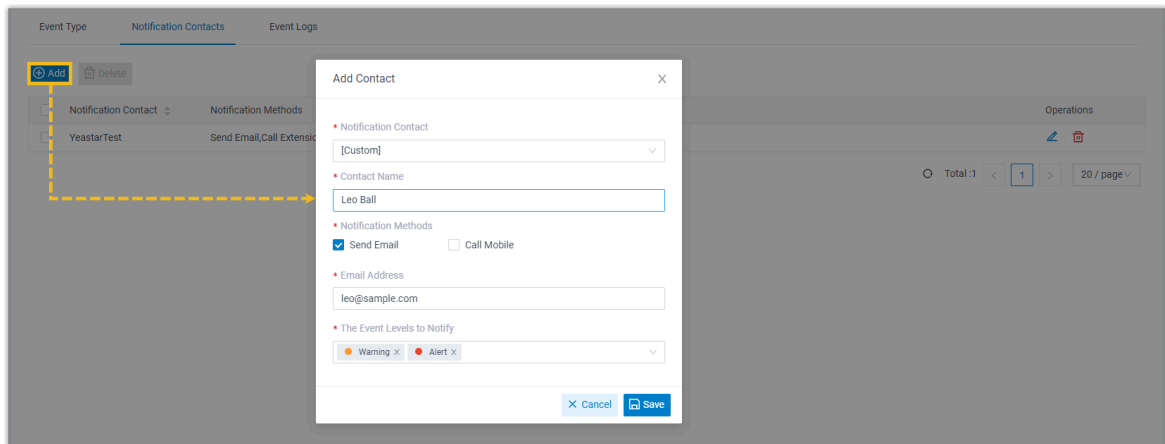
Yeastar P-Series PBX System supports to monitor and log system events, and notify relevant contacts when events occur.

You can control the events to monitor, the contacts to receive notifications, the way to notify (send email, call extension, or call mobile), as well as the content to send.

1. Go to **System > Event Notification**.
2. Under **Event Type** tab, turn on the notification of the desired events, and customize the event level and email template as needed.

Event Type			
Notification Contacts			
Event Logs			
Operations			
Event Name	Event Level	Notification	Email Template
Administrator Login Success	Information	<input type="checkbox"/>	<a href="#">✎</a>
Web User Login Success	Information	<input type="checkbox"/>	<a href="#">✎</a>
Web User Login Failed	Information	<input checked="" type="checkbox"/>	<a href="#">✎</a>
Linkus Client Login Failed	Information	<input checked="" type="checkbox"/>	<a href="#">✎</a>

3. Under **Notification Contacts** tab, add contacts to receive event notifications.



After receiving event notifications, you can check the details on PBX web portal (Path: **System > Event Notification > Event Logs**).

Event Type

Notification Contacts

Event Logs

Event Type

Event Level

Status

Event Name

Time

All

All

All

All

10/01/2023 00:00:00 ~ 10/12/2023 23:59:59

Download

Mark All as Read

Time	Event Type	Event Level	Event Name	Operations
10/11/2023 11:14:15	Operations	Information	Web User Login Failed	
10/10/2023 08:57:12	Telephony	Warning	SIP Trunk Registration Failed	
10/10/2023 08:56:03	System	Information	System Reboot	



### Note:

For detailed introduction and instruction about **Event Notification and Logging**, see [Event Notification Overview](#).

## Backup and Archive

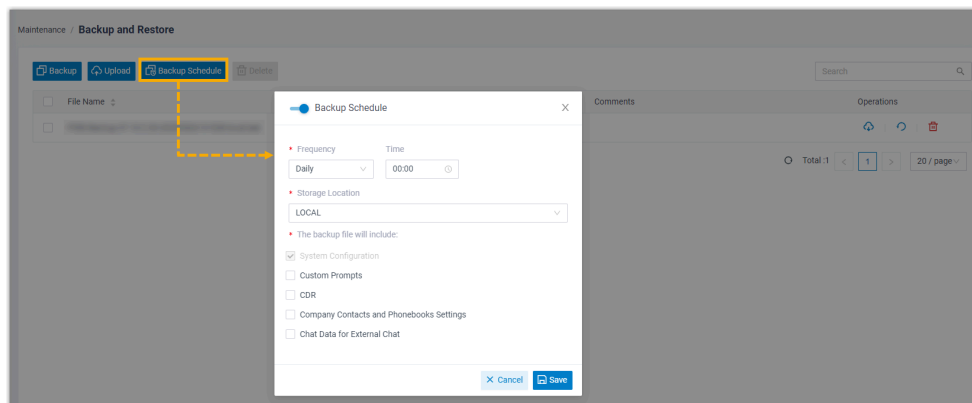
Yeastar P-Series PBX System allows you to back up the PBX's data and configurations, and even archive the backup files to external servers. This will help you minimize downtime and prevent data loss, ensuring business continuity in the event of a system failure.

### Back up PBX data and configuration

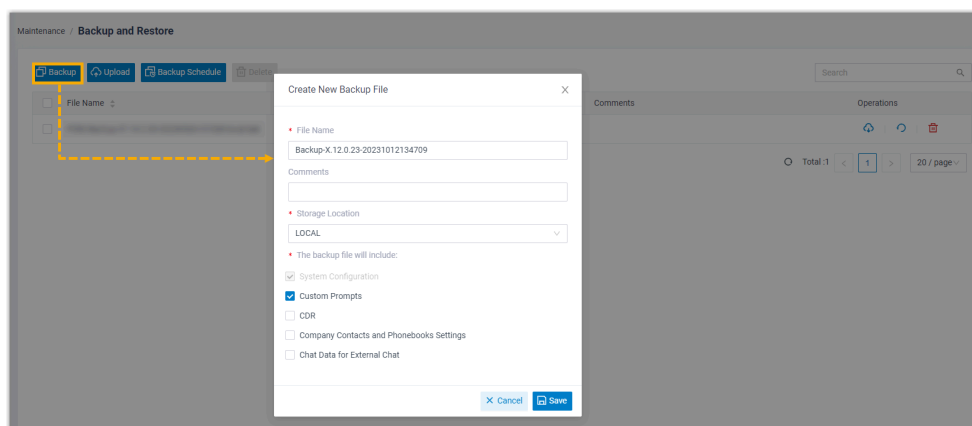
You can schedule automatic backups or create manual backups as needed.

1. Go to **Maintenance > Backup and Restore**.

2. To schedule automatic backups, click **Backup Schedule**, then set up and save the backup task.



3. To create a manual backup, click **Backup**, then choose the data and configurations to back up and save the backup task.



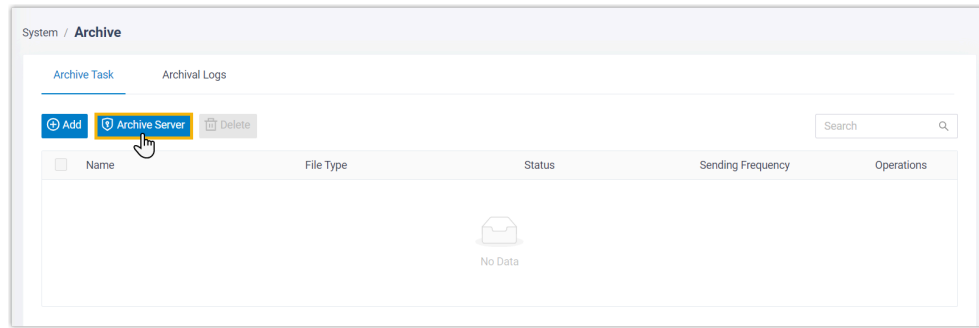
**Note:**

For detailed introduction and instruction about **Backup**, see [Overview of Backup and Restore](#).

## Archive backup files to external server

To provide an extra layer of protection for your backups, you can archive them to third-party storage such as **FTP Server**, **SFTP Server**, **S3-compatible Object Storage**, **Google Cloud Storage**, or **Microsoft SharePoint**.

1. Go to **System > Archive**.
2. Click **Archive Server** to add a archive server.



- [Add FTP server as archive server](#)
- [Add SFTP server as archive server](#)
- [Add S3-compatible object storage as archive server](#)
- [Add Google Cloud Storage bucket as archive server](#)
- [Add Microsoft SharePoint as archive server](#)

3. Click **Add** to create and set up an archive task.

