JumpServer

Quickstart

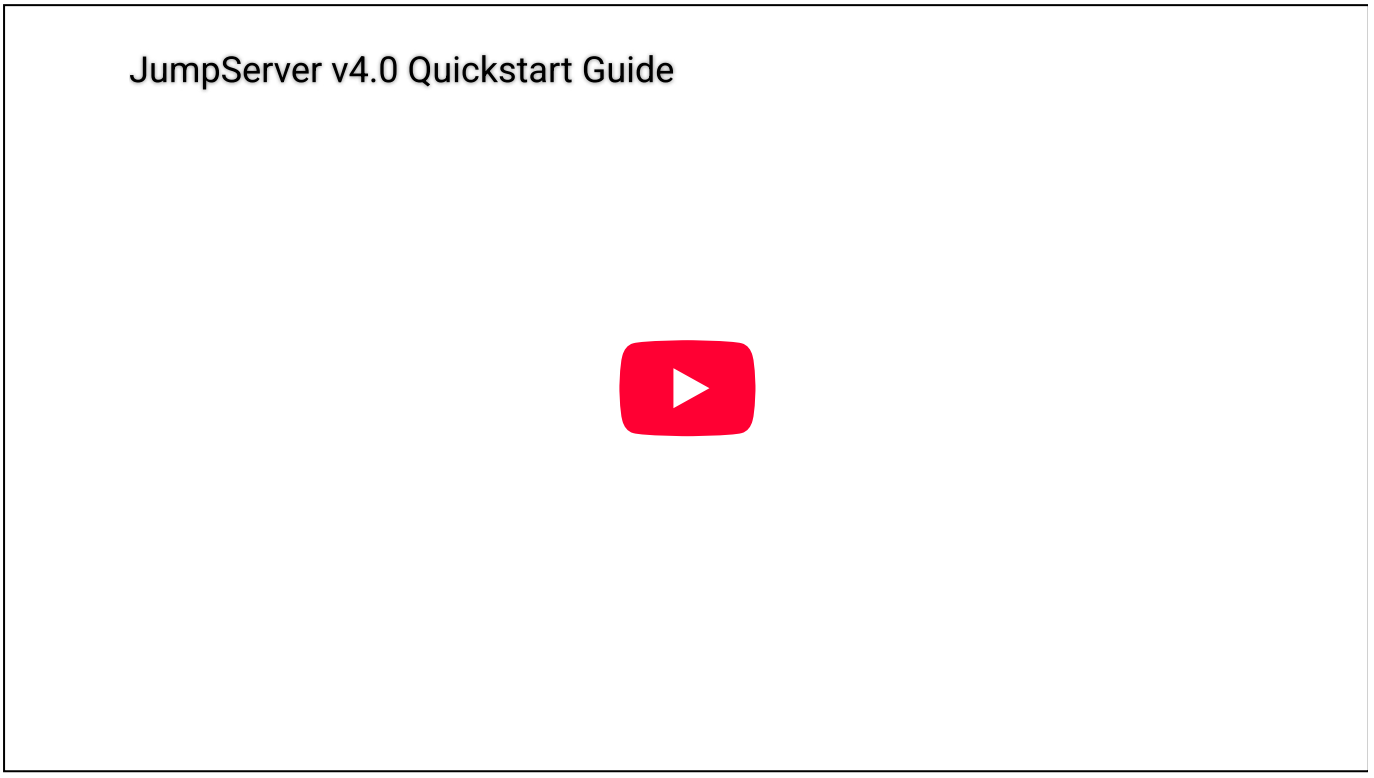
This topic walks you through JumpServer's features quickly and efficiently, helping you try them out in 10 minutes or less.

Introduction

For more information about JumpServer, see Introduction.

Next, we will complete the following steps: prerequisites, creating an asset, authorizing the asset to the Administrator, connecting to the asset via the web as the Administrator, and auditing sessions and commands.

You can watch the video below or follow the steps to quickly get started.

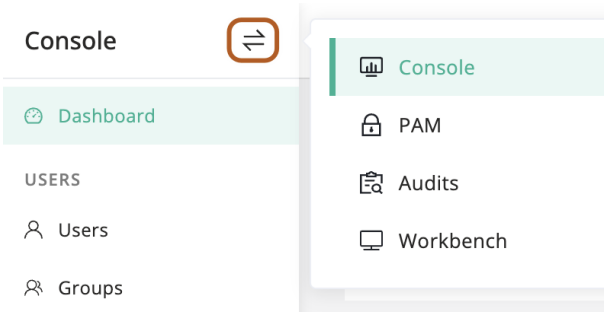


Prerequisites

Before starting, please install JumpServer, and **log in as an Administrator**. For more information, see Installation.

Creating an asset

1. At the top-left of the page, select ⇌, then click **Console**.



2. Navigate to the **Console** > **Assets** > **Host** tab.

3. Click **Create** to open the platform selection page on the right.

4. Select the **Linux** platform and open the asset creation page.

5. In the **Name** field, type a name for the asset, such as "Demo Linux".

6. In the **IP/Host** field, type the IP address of the asset, such as "172.16.10.110".

7. In the **Linux** field, keep the "Linux" platform selected.

8. In the **Nodes** field, select the "/DEFAULT" node.

9. In the **Accounts** field, click the **Add** and follow the steps in the pop-up to complete the account creation.

    1. In the **Name** field, type a name for the account, such as "root".

    2. In the **Username** field, type the username for the account, such as "root".

    3. In the **Secret type** field, select "Password".

    4. In the **Password** field, type the password for the account.

5. For other fields, keep the default values.

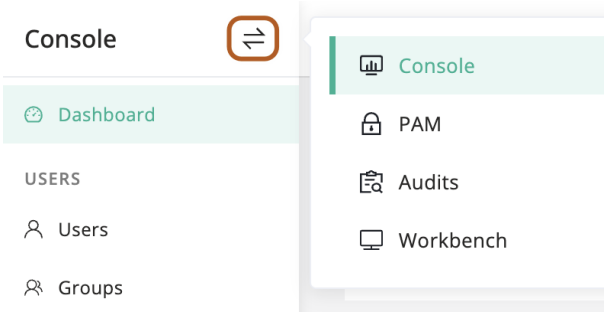
6. click **Confirm**.

10. For other fields, keep the default values.

11. Click **Submit**.

Authorizing asset for admin

1. At the top-left of the page, select ⇌, then click **Console**.



2. Navigate to the **Console** > **Authorization** page.

3. Click ＋**Create** to open the authorization creation form on the right-side page.

4. In the **Name** field, type a name for the authorization, such as "Authorize Demo Linux to Administrator".

5. In the **Users** field, select the "Administrator(admin)".

6. In the **Assets** field, select the "Demo Linux".

7. In the **Accounts** field, check only the box for "All existing accounts".

8. For other fields, keep the default values.

9. Click **Submit**.

Connecting to asset via web

1. In the right area of the top navigation bar, click .

2. At this point, the Web Terminal page should be open in a new browser tab.

   In the authorization tree on the left side, search for and click the "Demo Linux" asset.

3. An asset connection pop-up will appear, select connection parameters and establish the connection.

   1. Select the "SSH" tab, under the "Connect - Demo Linux".

   2. In the **Select account** section, Select "root".

   3. In the **Connect method** section, Select "Web > Web CLI".

   4. Click **CONNECT**.

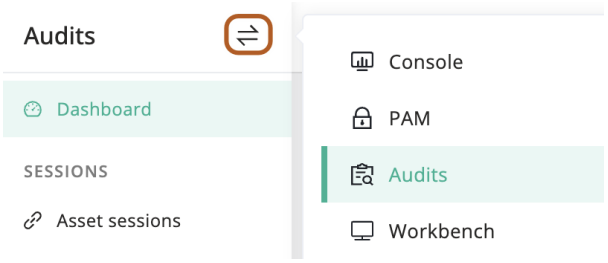
4. By this time, you should have successfully connected to the asset.

5. Next, you can try executing commands such as `ls -al`, `whoami` or `pwd`, etc.

6. Finally, run `exit` to end the current session.

Auditing connected sessions

1. At the top-left of the page, select , then click **Audits**.



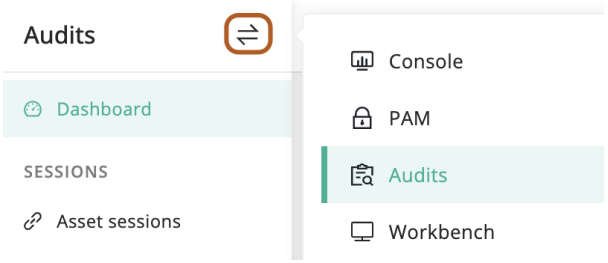
2. Navigate to the **Audits** > **Asset sessions** > **Historical sessions** tab.

3. You can view the history of asset connection sessions.

4. In the **Actions** column, click "Playback" to watch the recording online or "Download" to save it.

Auditing executed commands

1. At the top-left of the page, select , then click **Audits**.



2. Navigate to the **Audits** > **Session commands** page.

3. You can view all executed commands.

4. Click ⌄ at the end of the row to view the command result.

Next steps

Now that you've completed the quickstart guide, it’s time to explore more advanced features of JumpServer!

Last updated on August 15, 2025

Installation

This topic describes how to install JumpServer, including both the open-source and enterprise editions.

Install with a one-line command

This section introduces how to install the open-source version of JumpServer using a one-line command.

1. Prepare a clean Linux server (64bit, >= 4c8g).
2. Log in to the Linux server using the "root" or another user with superuser privileges.
3. Change to the `/opt` directory.
4. Run the command to install the latest open-source version of JumpServer.

```
curl -sSL https://github.com/jumpserver/jumpserver/releases/latest/download/quick_start.sh
| bash
```

5. After the installation is complete, open your Chrome browser and enter "http://<your-server-ip>" in the address bar.

> **Note**
>
> Replace `<your-server-ip>` with your actual server IP address.

6. Log in as an Administrator using the following default credentials.
    - username: `admin`

- password: `ChangeMe`

7. For security, you will be prompted to change your password after logging in. Once you've changed it and logged in again, you can start your JumpServer journey.

8. At this point, you have successfully installed JumpServer.

Install with an offline package

This section describes how to install the Enterprise Edition of JumpServer using an offline package.

1. Prepare a clean Linux server (64bit, >= 4c8g).

2. Log in to the Linux server using the "root" or another user with superuser privileges.

3. Change to the `/opt` directory.

4. Download the JumpServer Enterprise offline installation package.

Web **wget**

1. Log in to https://download-pkgs.jumpserver.com using the username and password provided by the support team.

2. Click filename to download the offline installation package for the required version.

3. Upload the offline installation package to the `/opt` directory on the deployment server.

5. Extract the offline installation package.

```
tar -zxvf jumpserver-ee-v4.10.13-x86_64.tar.gz
```

6. Change to the extracted directory.

```
cd jumpserver-ee-v4.10.13-x86_64
```

7. Perform the installation, the installation process can be completed using all default options. After the installation is complete, you can adjust the settings by modifying the configuration files.

```
./jmsctl.sh install
```

8. After the installation is complete, running `docker ps` will show the following three containers running:

   - jms_core
   - jms_postgresql
   - jms_redis

9. Start all services.

```
./jmsctl.sh start
```

10. Open your Chrome browser, enter "http://<your-server-ip>" in the address bar.

> **Note**
>
> Replace `<your-server-ip>` with your actual server IP address.

11. Log in as an Administrator using the following default credentials.

    - username: `admin`
    - password: `ChangeMe`

12. For security, you will be prompted to change your password after logging in. Once you've changed it and logged in again, you can start your JumpServer journey.

13. At this point, you have successfully installed JumpServer.

Next steps

- Import License: Learn how to import the enterprise edition license.
- Enable HTTPS: Learn how to enable HTTPS.
- Upgrade JumpServer: Learn how to upgrade JumpServer.

Last updated on November 20, 2025

Upgrade

This topic describes how to upgrade JumpServer, including both the open-source and enterprise editions.

> **Tip**
>
> We recommend upgrading JumpServer regularly to access the latest designs and features.

Upgrade for one-line installation

If you have installed JumpServer using the Install with a one-line command guide, you can upgrade JumpServer by running the following steps.

1. Log in to the JumpServer deployment server using the "root" or another user with superuser privileges.
2. Change to the `/opt` directory.
3. Download the latest installation package.

```
wget https://github.com/jumpserver/installer/releases/download/v4.10.13/jumpserver-installer-v4.10.13.tar.gz
```

4. Extract the installation package.

```
tar -zxvf jumpserver-installer-v4.10.13.tar.gz
```

5. Change to the extracted directory.

```
cd jumpserver-installer-v4.10.13
```

6. Perform the upgrade.

```
./jmsctl.sh upgrade
```

7. Start all services.

```
./jmsctl.sh start
```

8. At this point, you have successfully upgraded JumpServer.

Upgrade for offline installation

If you have installed JumpServer using the Install with an offline package guide, you can upgrade JumpServer by running the following steps.

1. Log in to the JumpServer deployment server using the "root" or another user with superuser privileges.
2. Change to the `/opt` directory.
3. Download the JumpServer Enterprise offline installation package.

Web **wget**

1. Log in to https://download-pkgs.jumpserver.com using the username and password provided by the support team.
2. Click filename to download the offline installation package for the required version.
3. Upload the offline installation package to the `/opt` directory on the deployment server.

4. Extract the installation package.

```
tar -zxvf jumpserver-ee-v4.10.13-x86_64.tar.gz
```

5. Change to the extracted directory.

```
cd jumpserver-ee-v4.10.13-x86_64
```

6. Perform the upgrade, the upgrade process can be completed using all default options.

```
./jmsctl.sh upgrade
```

7. Start all services.

```
./jmsctl.sh start
```

8. At this point, you have successfully upgraded JumpServer.

Last updated on November 20, 2025

Create user

About user

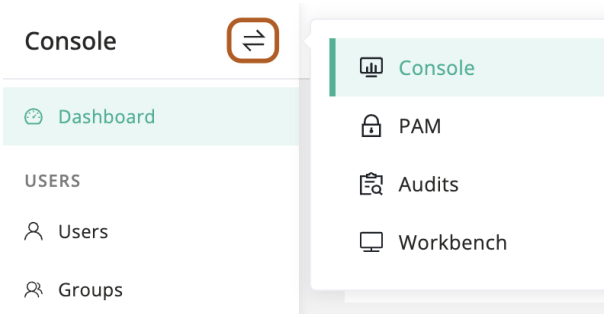
In JumpServer, **User** is a core entity of the system, used for logging in and accessing assets, and also serves as the fundamental object for administrators to grant resource permissions.

All users are unique globally and can be assigned multiple system roles, thereby inheriting the corresponding system-level permissions.

In the Enterprise edition, a user can belong to multiple organizations and have multiple organization roles, enabling fine-grained permission control across or within organizations.

Create a user

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, under the USERS section, click **Users**.

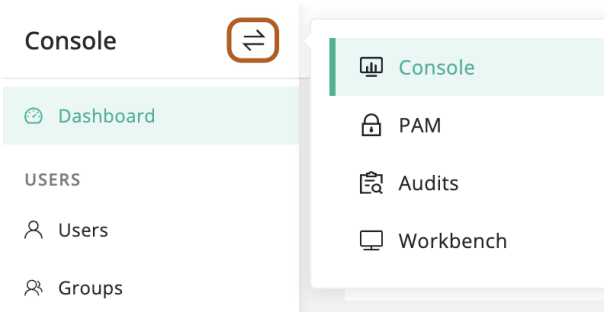
3. Click **+ Create**.

4. Type user information. About user parameters, see User parameters reference.

5. Click **Submit**.

Duplicate a user

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, under the USERS section, click **Users**.

3. In the user table, find the user that you want to duplicate.

4. In the Actions column, click the ··· icon, then click **Duplicate**.

5. Modify user information, including at least the Name, Username, and Email.

6. Click **Submit**.

User parameter reference

Name

`required`

The name is used to identify a user.

Username

`required` `unique`

The username is used to log in to JumpServer.

Email

`required` `unique`

The user email is primarily used to receive system notifications. It also supports the following functions:

- Users can use their email as the username to log in to JumpServer.
- Used for password recovery.
- Serves as a method for multi-factor authentication (MFA) and receive MFA codes.

> **Tip**
>
> For more information about configuring the email service, see Email service configuration guide.

> **Tip**
>
> For more information on using Email as an MFA method, see MFA via email.

Groups

User groups are used for organizing and managing users. A user can belong to multiple groups.

Password setting

(Create local user only) Choose the method for setting the password for a newly created user.

- Reset link will be generated and sent to the user

  This will send a password setup email to the user. The user can log in after resetting the password as instructed.

- Set password

  Manually set password. The user can log in directly with this password.

Change secret

(Edit local user only) When editing a user, check to update the user's password.

Password

(Local user only) The user can log in to the system using this password.

Password rules can be configured in the system settings, including requirements for length, uppercase and lowercase letters, numbers, and special characters.

When `Password must be changed during next login` is checked, the user will be required to change the password immediately after the first successful login.

MFA

Configure the Multi-Factor Authentication (MFA) policy for a single user.

- Disabled

  MFA is disabled by default, but users can enable it from their profile page.

- Enabled

  MFA is enabled for the user, but they can disable it from their profile page.

- Force enabled

  MFA is enforced for the user, and they cannot disable it.

You can also configure a global MFA policy in the system settings. For more information, see Global MFA.

MFA supports the following methods:

- One-Time Password (OTP)
- SMS
- Email
- Passkey
- Facial recognition

Source

User source identifies the user authentication backend. JumpServer supports integrating and enabling multiple authentication services simultaneously. When the same user exists in multiple services, this field helps distinguish the user's source. **Local** user belongs to the local database.

When a user logs in, the system will, by default, authenticate them using all enabled backends sequentially. Administrators can also configure the system to allow authentication only from the user's source, which helps improve authentication efficiency.

System roles

`required`

System roles define a user's position in the system and grant only the permissions assigned to each role. Multiple system roles can be assigned, with permissions combined.

Built-in roles include:

- User
- System Admin
- System Auditor

> **Enterprise**
>
> A system role grants the user all permissions across all organizations. Administrators can also create custom system roles.

Organization roles

`required`

(Enterprise only) Organization roles define a user's position within the current organization and grant only the permissions assigned to each role. Multiple organization roles can be assigned, with permissions combined.

Built-in roles include:

- User

- Organization Admin
- Organization Auditor

You can click **Manage role** to view existing roles or create new ones.

Active

Active controls the user's activation status. Being active is one of the requirements for logging into the system.

Additionally, the administrator can configure in System Settings to automatically disable users who have not logged in for an extended period. For more information, see Auto disable threshold (day).

Date expired

You can set a future expiration date for a user in advance. Once the user expires, they can't log in to JumpServer.

You can also set the default expiration days for new users in the configuration file. For more information, see USER_DEFAULT_EXPIRED_DAYS.

Phone

The user's mobile phone number can be used to receive MFA codes.

Description

Additional descriptive information about the user.

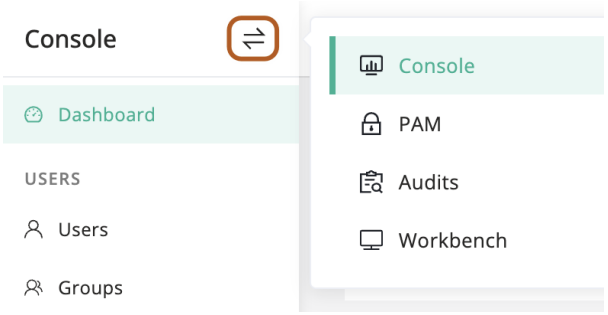
Last updated on November 10, 2025

Edit user

The edit user feature is used to modify user information, manage permissions, and control account status, helping administrators easily maintain users and manage system access.

Edit a user

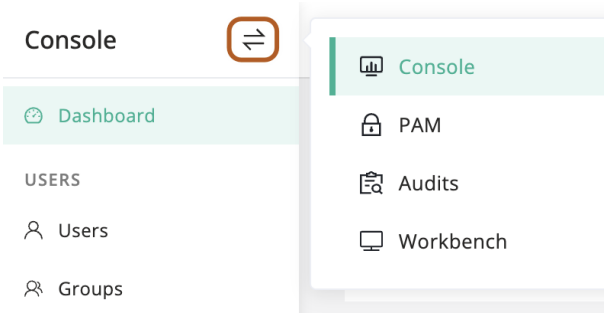
1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, under the USERS section, click **Users**.
3. In the user table, find the user that you want to edit.
4. In the Actions column, click **Edit**.
5. Modify user information. About user parameters, see User parameters reference.
6. Click **Submit**.

Bulk edit users

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, check the users you want to edit.

4. Above the table, select **Actions** button, then click **Edit selected**.

Last updated on November 10, 2025

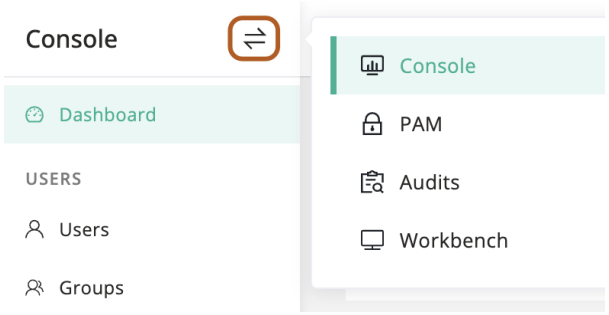
Delete users

> **Tip**
>
> If you only want to temporarily prevent a user from logging in, please refer to Enable or disable users.

> **Warning**
>
> Deleting a user will also remove all associated authorizations and cannot be undone. Please confirm before proceeding.

Delete a user

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

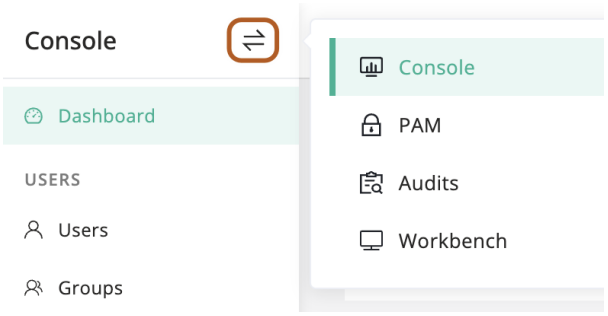
3. In the user table, find the user that you want to delete.

4. In the Actions column, click the ··· icon, then click **Delete**.

5. Confirm the information and click **OK**.

Bulk delete users

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, check the users you want to delete.

4. Above the table, select **Actions** button, then click **Delete selected**.

5. Confirm the information and click **OK**.

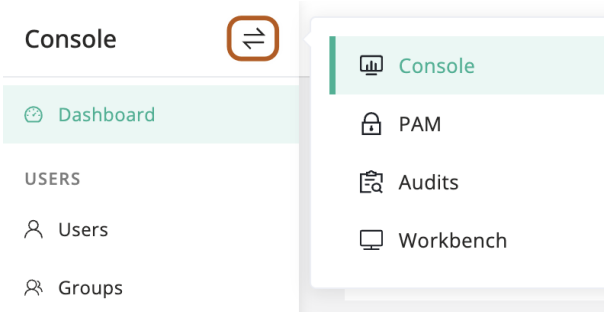
Last updated on August 21, 2025

Enable or disable users

For security, users who haven't logged in for a long time are disabled. For more information about the configuration guide, see Auto disable threshold (day).

Enable or disable a user

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

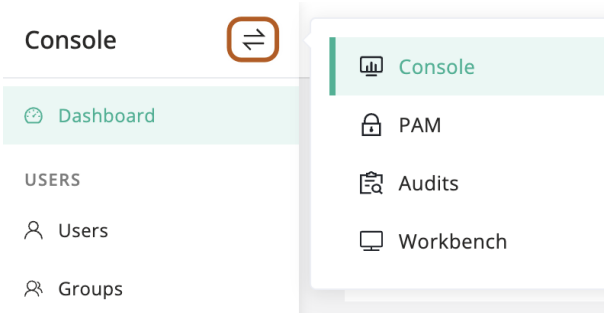
3. In the user table, click the name of the user you want to enable or disable.

4. On the user details page, click **Basic** tab.

5. In the Quick update card, turn on/off the "Active" toggle to **enable** or **disable** the user.

Bulk enable or disable users

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, check the users you want to enable or disable.

4. Above the table, select **Actions** button, then click **Activate selected** or **Disable selected**.

Last updated on August 22, 2025

Invite or remove user from an organization

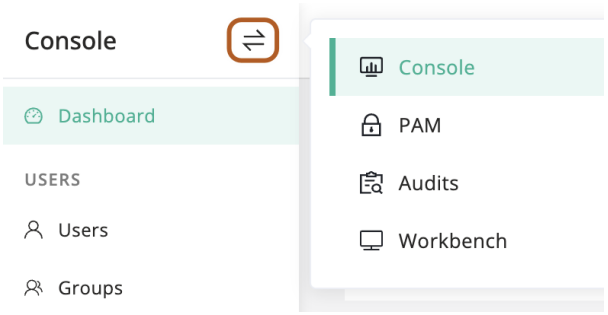
In the Enterprise edition, you can invite a user from one organization to another and assign them specific roles. The user will automatically inherit the permissions associated with those roles in the new organization.

Removing a user from an organization will revoke their access but will not delete the user.

Bulk invite users to the current organization

1. In the left area of the top navigation bar, click the organization dropdown and switch to the target organization.

2. At the top-left of the page, select ⇌, then click **Console**.



3. In the left menu, click **Users**.

4. Above the user table, Click **Invite**.

5. In the **Users** field, select one or more users to invite.

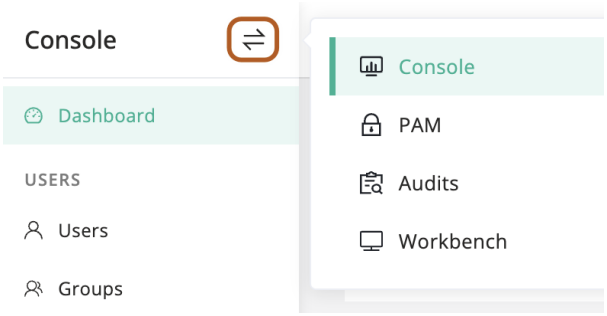
6. In the **Org roles** field, select one or more organization roles.

7. Click **Confirm**.

Remove a user from the current organization

1. In the left area of the top navigation bar, click the organization dropdown and switch to the target organization.

2. At the top-left of the page, select ⇌, then click **Console**.



3. In the left menu, click **Users**.

4. In the user table, find the user you want to remove.

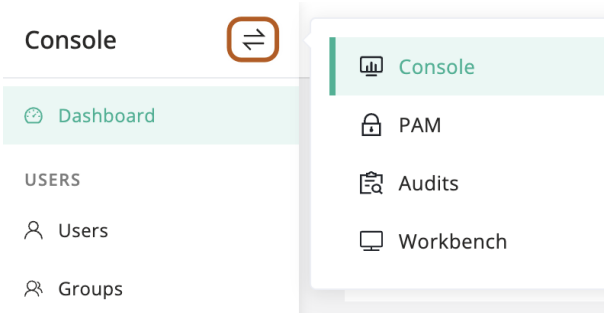
5. In the Actions column, click the ··· icon, then click **Remove**.

6. Confirm the information and click **OK**.

Bulk remove users from the current organization

1. In the left area of the top navigation bar, click the organization dropdown and switch to the target organization.

2. At the top-left of the page, select ⇌, then click **Console**.



3. In the left menu, click **Users**.

4. In the user table, check the users you want to remove.

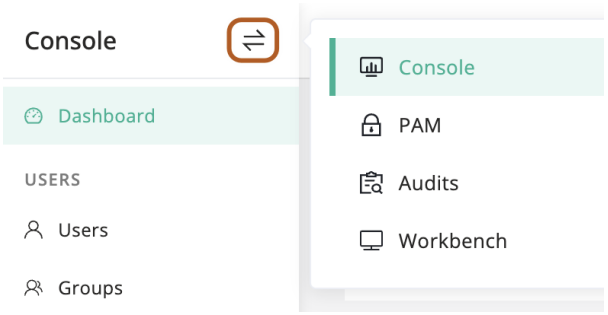
5. Above the user table, select **Actions** button, then click **Remove selected**.

Last updated on August 20, 2025

Unlock user

When a user fails to log in many times within a short period, the system temporarily locks the user to enhance security and prevent brute-force attacks. The administrator can unlock the user.

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to unlock.

4. On the user details page, click **Basic** tab.

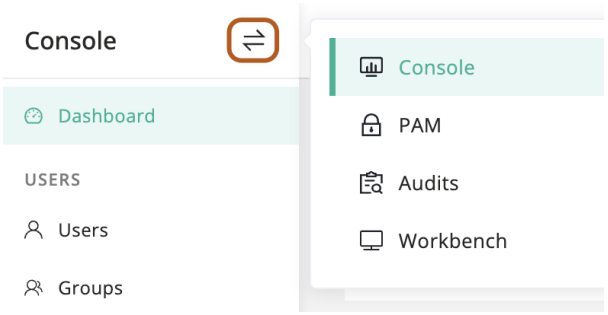
5. In the Quick update card, find the "Unlock user" section and click **Unlock**.

Last updated on August 20, 2025

Reset user password

When a user forgets their password and cannot log in, the administrator can reset the password by sending a reset email. The user can then set a new login password.

1. At the top-left of the page, select ⇌, then click **Console**.



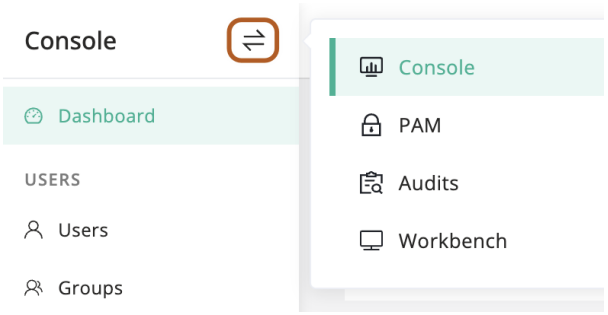
2. In the left menu, click **Users**.
3. In the user table, click the name of the user you want to reset.
4. On the user details page, click **Basic** tab.
5. In the Quick update card, find the "Reset password" section and click **Send**.
6. Confirm the information and click **OK**.
7. A reset password email will be sent to the user by the system.
8. In the email, the user clicks the **Click here reset password** link to open the password reset page.
9. Type a new password and confirm it, then click **Submit**.
10. The user will receive a password reset success notification email.

Last updated on August 20, 2025

Reset user SSH Key

Reset user SSH Key does not directly reset the key. It only sends an email to the user with instructions on how to set up their SSH Key.

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to reset.

4. On the user details page, click **Basic** tab.

5. In the Quick update card, find the "Reset ssh key" section and click **Send**.

6. Confirm the information and click **OK**.

7. A reset SSH key email will be sent to the user by the system.

8. In the email, the user clicks the **Click here set** link to open the SSH key page.

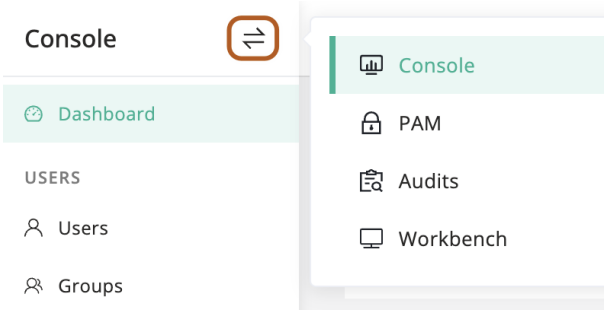
9. The user can add or delete SSH keys.

Last updated on August 20, 2025

Reset user MFA

When a user cannot log in due to a lost MFA, the administrator can reset MFA for the user.

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to reset.

4. On the user details page, click **Basic** tab.

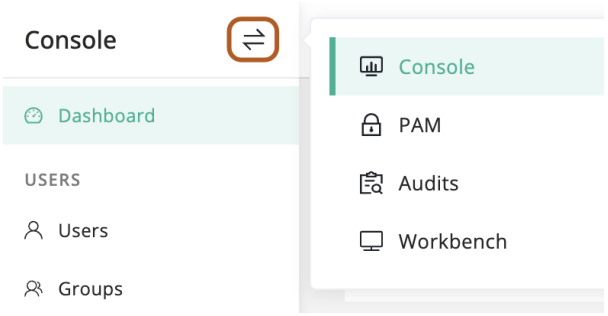
5. In the Quick update card, find the "Reset mfa" section and click **Reset**.

Last updated on August 20, 2025

View user related resources

View assets authorized to the user

1. At the top-left of the page, select ⇌, then click **Console**.



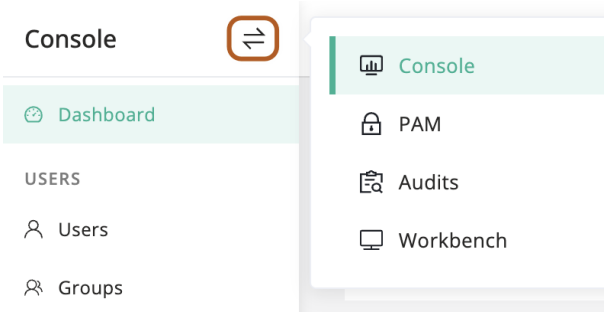
2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to view.

4. On the user details page, click **Authorized assets** tab.

View the user's authorizations

1. At the top-left of the page, select ⇌, then click **Console**.



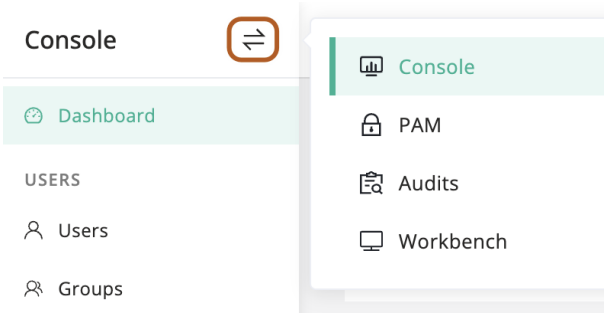
2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to view.

4. On the user details page, click **Authorization rules** tab.

View the user's asset sessions

1. At the top-left of the page, select ⇌, then click **Console**.



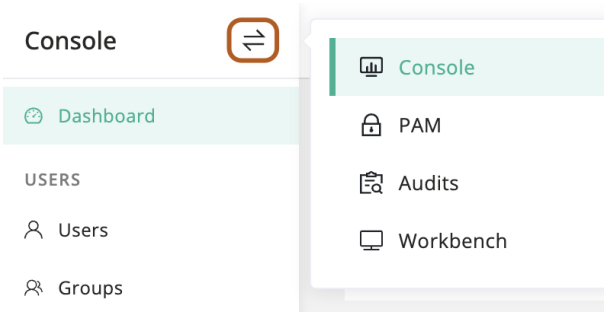
2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to view.

4. On the user details page, click **Asset sessions** tab.

View the user's activity logs

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to view.

4. On the user details page, click **Activities** tab.

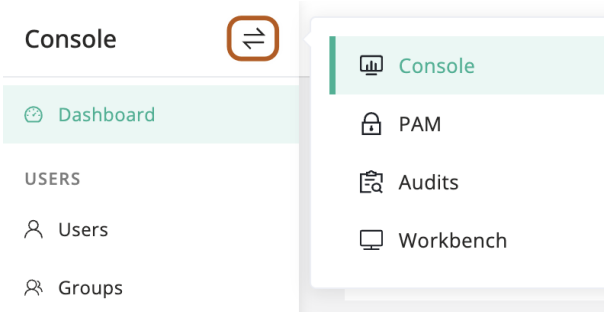
Last updated on November 6, 2025

User login ACL

Only system administrators have permission to manage users' Login ACLs.

Create user login ACL

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Users**.

3. In the user table, click the name of the user you want to manage.

4. On the user details page, click **Login ACLs** tab.

5. Click **+ Create**.

6. Type the login ACL information. About login ACL parameters, see Login ACL parameters reference.

7. Click **Submit**.

Login ACL parameter reference

Name

The name of the login ACL.

Priority

The priority of the login ACL. A lower value indicates a higher priority.

User

The user to whom the login ACL applies.

- All users: The login ACL applies to all users.
- Specified user: The login ACL applies to the specified user.
- Filter by attribute: The login ACL applies to users filtered by the specified attribute.

IP

The IP address or IP address range to which the login ACL applies. You can specify multiple IP addresses or IP address ranges.

`*` indicates all IP addresses.

Time period

The time period during which the login ACL is effective. You can specify multiple time periods.

Action

The action to be taken when the login ACL is matched.

- Reject: Deny the user login.
- Accept: Allow the user login.
- Review: Require manual review for the user login.

- Notify: Send notifications to the configured recipients for user login events.

Active

Specifies whether the login ACL is active.

Description

The description of the login ACL.

Last updated on November 10, 2025

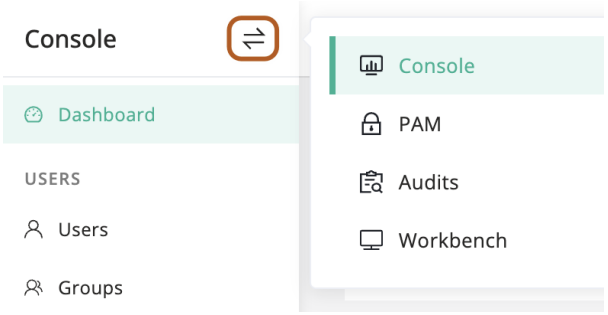
Create group

About group

In JumpServer, a group is a collection of users who share common characteristics or roles. Groups help administrators efficiently manage permissions, access control, and resource allocation by organizing users into logical units.

Create group

1. At the top-left of the page, select ⇄, then click **Console**.



2. In the left menu, under the USERS section, click **Groups**.

3. Click **+ Create**.

4. In the **Name** field, type group name.

5. In the **Users** field, select users to be added to the group.

6. In the **Description** field, type a description for the group.

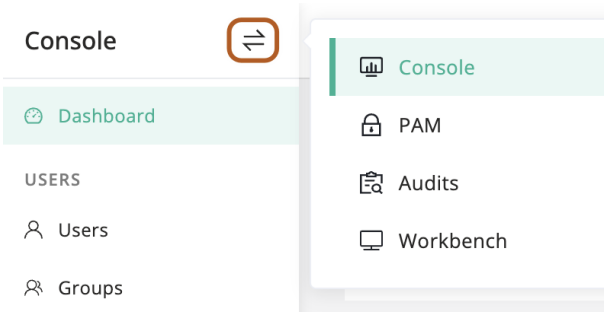
7. Click **Submit**.

Last updated on November 10, 2025

View users in the group

You can view all users belonging to a specific group in JumpServer. This helps administrators manage group memberships and ensure that users have the appropriate access and permissions based on their group affiliations.

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, under the USERS section, click **Groups**.

3. In the group table, click the name of the group whose users you want to view.

4. On the group details page, click the **Users** tab to see the list of users in the group.

Last updated on November 10, 2025

Create a web asset

About web asset

Web assets are a type of resource supported by JumpServer, designed for accessing web systems through remote applications. They are suitable for centrally managing internal systems, SaaS services, or other web-based applications.

Web assets rely on remote application publishers, which can be deployed on either Windows or Linux systems.

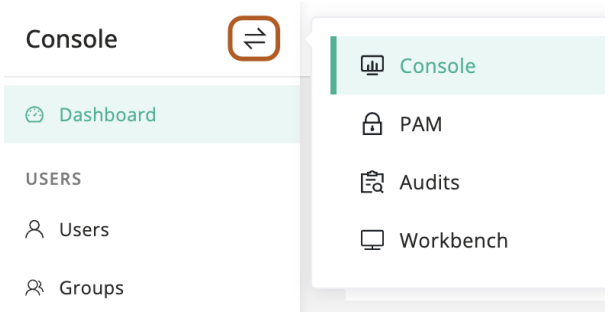
When a user connects to a web asset, the system automatically calls the publisher to launch a preconfigured browser that accesses the target system. This approach enables secure and controlled access, effectively preventing users from directly accessing the target address.

Prerequisites

- You must have created at least one **RemoteApp machine** or an **VirtualApp publisher**.

Create a web asset

1. At the top-left of the page, select ⇌, then click **Console**.



2. In the left menu, click **Assets**.

3. On the right page, click **Web** tab.

4. Above the table, click **Create**, or the  to its right.

5. Select the Website platform.

6. Type a name for the website.

7. Type the website URL, include the port number if it is not 80 or 443.

8. Select one or more nodes.

9. Choose a autofill method. For more information, see About autofill.

10. Optionally, add accounts manually or from a template.

11. Optionally, select only one zone.

12. Optionally, select one or more tags.

13. Optionally, type a description for the website.

14. Click **Submit** or **Save & Continue**.

About autofill

The autofill feature is mainly used for websites that require user authentication. Before the user accesses such a website, JumpServer automatically fills in the predefined username and password on the login page to complete authentication. This process is transparent to the user, requiring no manual input of credentials.

1. Disabled

This disabled method is intended for websites that do not require authentication.

2. Basic

The basic method is suitable for websites where the username, password, and login button are all on the same page. JumpServer automatically fills in the credentials and submits the form to authenticate the user.

When auto-filling information, it is necessary to locate elements on the web page. The supported selector types include Name selectors, ID selectors, Class selectors, CSS selectors, and XPath selectors. For more information, see Selenium Python: Locating Elements.

3. Script

This script method is intended for websites with complex login procedures. It supports advanced automation, including multi-step authentication and interaction with dynamic page elements.

Script structure

The script here is an array, where each element is a dictionary, representing a step in the script. Each step contains the following keys:

Key	Required	Type	Description
`step`	Yes	Integer	Indicates the execution order of the script, starting from 1 and increasing sequentially.
`value`	Yes	String	Built-in variables supported: `{USERNAME}`, `{SECRET}`. If the command is not type, leave the value as an empty string.
`target`	Yes	String	The target element to be operated on, which can be a selector or an XPath expression.
`command`	Yes	String	The command to be executed, which can be one of the following: click, type, sleep, select_frame.

command options:

Command	Description
`click`	Click the target element.
`type`	Type the value into the target element.
`sleep`	Pause the script for a specified duration, typically to allow page loading during navigation. The duration is specified by target, in seconds.
`select_frame`	Switch to the specified iframe for operations. The target supports options like `id=iframe_id`, `name=iframe_name`, or `index=1`. If `index < 0`, it switches back to the `default`/`main` iframe).

Script example

1. Switch to the iframe with `id=iframe_id`.
2. Type the username into the input field with `name=username`. The `{USERNAME}` variable will be replaced with the actual username when the script is executed.
3. Click the next button to proceed to the next step in the login process.
4. Pause the script for 5 seconds to allow the next page to load.
5. Type the password into the input field with `name=password`. The `{SECRET}` variable will be replaced with the actual password when the script is executed.
6. Click the submit button to complete the login process.

```
[
  {
      "step": 1,
      "command": "select_frame",
      "target": "id=iframe_id",
      "value": ""
  },
  {
      "step": 2,
      "command": "type",
      "target": "name=username",
      "value": "{USERNAME}"
  },
  {
      "step": 3,
      "command": "click",
      "target": "id=next_button",
      "value": ""
  },
  {
      "step": 4,
      "command": "sleep",
      "target": "5",
      "value": ""
  },
  {
      "step": 5,
      "command": "type",
      "target": "name=password",
      "value": "{SECRET}"
  },
  {
      "step": 6,
      "command": "click",
      "target": "id=submit_button",
      "value": ""
  }
]
```

Last updated on December 2, 2025

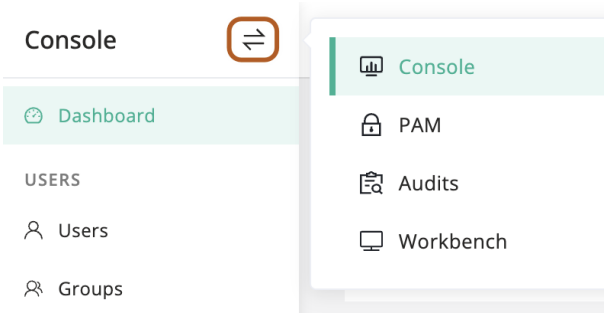
Import and export resources

This topic describes how to import and export resources, currently supporting "CSV" and "Excel" formats. Resource import includes "Import for creation" and "Import for update".

The steps for importing and exporting are the same, except for the field definitions of different resource types. For more information, see Resource Attributes.

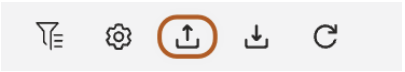
Create resources by importing

1. At the top-left of the page, select ⇌, then click **Console**.



2. Navigate to the "Resources" page.

3. In the top-right corner of the "Resources" table, click ↑.



4. At this point, a pop-up window will appear.

5. In the **Import** section, choose "Create".

6. After the "Download creation template", click CSV or XLSX to download the template.

7. Add the resources you want to create to the template.

> **Tip**
>
> For more information about resource field definitions, see Resource Attributes.

8. In the **Upload** section, click "Drag files here, or click to upload" to select the template you have edited.

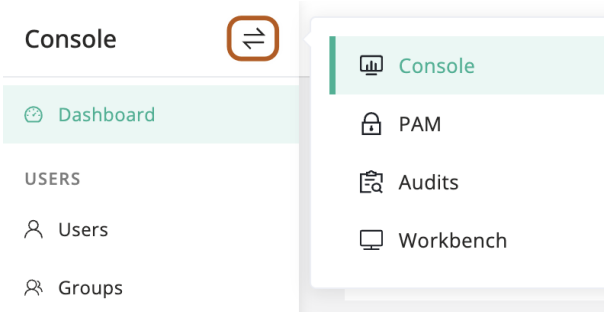
9. The resource data will appear in the table. Double-click an entry to edit.

10. Click **Import** button to begin the import.

> **Warning**
>
> For import errors, see Troubleshooting Import Failures.

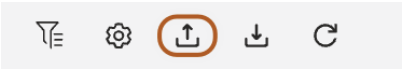
Update resources by importing

1. At the top-left of the page, select ⇌, then click **Console**.



2. Navigate to the "Resources" page.

3. In the top-right corner of the "Resources" table, click ⬆.



4. At this point, a pop-up window will appear.

5. In the **Import** section, choose "Update".

6. After the "Download update template", click CSV or XLSX to download the template.

7. Add the resources you want to update to the template. Make sure each entry includes an "ID".

> **Note**
>
> We recommend exporting the resources you want to update, copying their information into the template, making the necessary changes, and then importing it to update. For export guides, see Export resources.

> **Tip**
>
> For more information about resource field definitions, see Resource Attributes.

8. In the **Upload** section, click "Drag files here, or click to upload" to select the template you have edited.

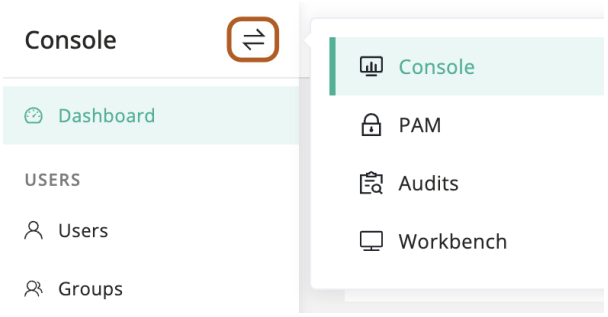
9. The resource data will appear in the table. Double-click an entry to edit.

10. Click **Import** button to start the import.

> **Warning**
>
> For import errors, see Troubleshooting Import Failures.

Export resources

1. At the top-left of the page, select ⇄, then click **Console**.



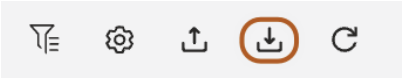
2. Navigate to the "Resources" page.

3. Perform the corresponding action based on the export scope you want.

Export all | **Export selected items** | **Export filtered items**

No action required, proceed directly to the next step.

4. In the top-right corner of the "Resources" table, click .



5. At this point, a pop-up window will appear.

6. In the **File type** section, choose "CSV" or "Excel" as the export format.

7. In the **Export range** section, choose the scope you want to export.

8. Click **Confirm** button to start the export.

Troubleshooting

Import failure

If there are import failures, follow the steps below to fix them and continue the import.

1. At the top left of the table, click **Failed** tab to show only the failed entries.

2. In the **Status** column, hover over the ❌ to check the failure reason.

3. After correcting all the erroneous fields, click **Continue**.

Resource attributes

Click the resource name to view the field definitions for each resource, helping you add resources to the file more accurately.

- Users

Last updated on August 11, 2025

User attributes description

This topic describes the attributes related to user import.

Attribute	Type	Description
ID	UUID	Length of 36 Required only during import update
* Name	Text	Max length 128
* Username	Text	Max length 128
* Email	Text	Max length 128
Password setting	Choices	Options: email: User sets password via email custom: Custom password will be set
Password	Text	Max length 128
Public Key	Text	-
Source	Choices	Options: local, ldap, ldap_ha, openid, radius, cas, saml2, oauth2, wecom, dingtalk, lark, slack, feishu, custom
MFA	Choices	Options: 0: Disabled 1: Enabled 2: Force enabled
Groups	List	Example: ["GroupID", ...]
Org Roles	List	Example: ["OrgRoleID", ...]
System Roles	List	Example: ["SystemRoleID", ...]
Tags	List	Example: ["TagName:TagValue", ...]

Attribute	Type	Description
		If the label does not exist, it will be created automatically
WeChat	Text	Max length 256
Phone	Text	-
Need update password	Boolean	Yes/No
Active	Boolean	Yes/No
Date expired	Date	Format: YYYY/MM/DD HH:mm:ss +0000
Updated By	Text	Max length 30
Description	Text	-

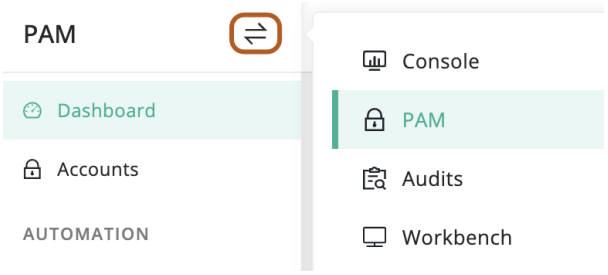
Last updated on April 30, 2025

Create account discovery task

Account Discovery refers to the automatic identification of accounts on servers. The system supports syncing discovered accounts to JumpServer and associating accounts with corresponding assets.

Before starting account discovery, you need to create a **high-privilege** account for the asset, because JumpServer will use this account to retrieve other accounts during task execution.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Discover accounts**.

3. On the right page, click **Account discovery tasks** tab.

4. Click **+ Create**.

5. In the **Name** field, type the task name.

6. Optionally. In the **Nodes** field, select one or more nodes. The task will execute account discovery on all assets under the selected nodes and their subnodes.

7. Optionally. In the **Assets** field, select one or more assets.

8. Check **Sync to Assets** to synchronize the discovered accounts to the asset accounts.

9. Check **Check risk** to scan discovered accounts for risks.

10. Optionally. In the **Recipient** field, select one or more recipients. Upon completion of each execution, the task result will be delivered via email.

11. Check **Periodic** to enable scheduled execution.

12. Choose either **Crontab** or type **Interval** (in hours) to set the task execution schedule. Crontab has higher priority than Interval, so only one needs to be configured.

13. In the **Active** field, check to enable the task.

14. In the **Description** field, type the task description.

15. Click **Submit**.

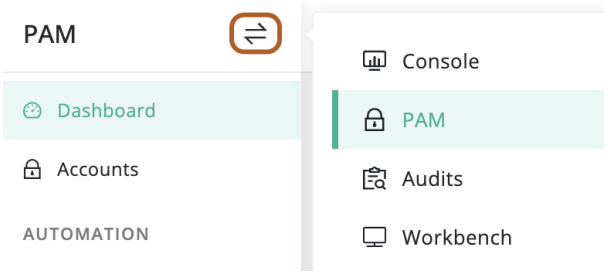
Last updated on August 5, 2025

Create push account task

Account push means sending local account information from the JumpServer to remote hosts automatically. This helps create or update accounts on multiple hosts without manual login. Pushed content includes account name, password or private key.

Before starting account push, create a high-privilege account for the asset. JumpServer uses this account to create other accounts during task execution.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Push accounts**.

3. On the right page, click the **Account push tasks** tab.

4. Click **+ Create**.

5. In the **Name** field, type the task name.

6. Optionally. In the **Nodes** field, select one or more nodes. The task will execute account push on all assets under the selected nodes and their subnodes.

7. Optionally. In the **Assets** field, select one or more assets.

8. In the **Accounts** field, type one or more account usernames to push to the assets.

> **Note**

If the account exists on the asset, its secret will be used. Otherwise, the account will be created using the task's secret strategy and pushed.

9. In the **Secret strategy** field, you can choose "Specific secret" to set it manually, or "Random generate" to generate it randomly.

10. In the **Secret type** field, you can choose either "Password" or "SSH key".

11. In the **Password** field, type a password. (Specific secret & Password)

12. In the **Private key** field, paste your private key. (Specific secret & SSH key)

13. In the **Key password** field, type the private key password. (Specific secret & SSH key)

14. In the **Password rules** field, set password rules, including length, uppercase and lowercase letters, numbers, special characters, and excluded characters. (Random generate & Password)

15. In the **Push parameters** field, you can configure push parameters.

> **Note**
>
> You can configure push parameters only when a Host-type asset or a node containing Host-type assets is selected.

16. In the **Periodic** field, check to enable scheduled execution.

17. In the **Check connection after change** field, check to verify the connection after the push task is completed.

18. In the **Active** field, check to enable the task.

19. In the **Description** field, type the task description.

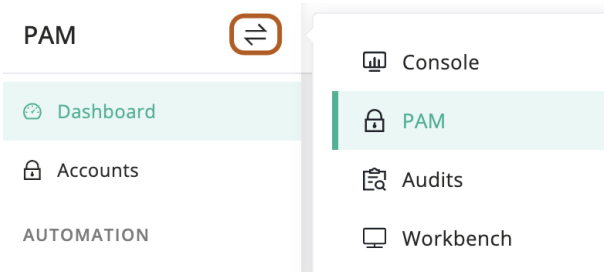
20. Click **Submit**.

Last updated on August 15, 2025

Create account backup task

Account backup saves local account information and supports unified backup across different asset types. Backups can be stored via Email or SFTP, with optional scheduled backup and password splitting to separate recipients or SFTP servers.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Backup accounts**.

3. On the right page, click the **Account backup tasks** tab.

4. Click **+ Create**.

5. In the **Name** field, type the task name.

6. In the **Type** field, check asset categories or asset types to be backed up.

7. In the **Backup type** field, choose how to store the backup.

   - `Email`: Send the backup file via email.
   - `SFTP`: Send the backup file to the SFTP server.

8. In the **Password divided** field, check and enable password-splitting backup. The account password will be split into two parts and sent separately to two groups of recipients.

9. In the **Recipient a/b**, select one or two recipient groups separately. The backup file will be encrypted using the file encryption password set in the personal settings by default (via email).

10. In the **Receiving server a/b** field, select one or two receiving servers. The backup file will be encrypted using the "Zip encrypt password" (via SFTP).

11. In the **Zip encrypt password** field, type the password to encrypt the backup file (via SFTP).

12. In the **Periodic** field, check to enable scheduled execution.

13. In the **Active** field, check to enable the task.

14. In the **Description** field, type the task description.

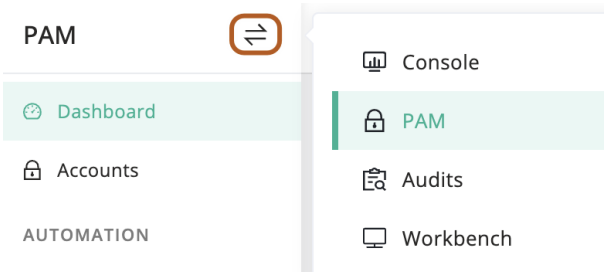
15. Click **Submit**.

Last updated on August 11, 2025

Create account secret change task

Change secrets refers to bulk modification of account login secrets and keys on hosts. Enables centralized management across multiple asset accounts, with custom rotation cycles and optional email notifications for task results.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Change secrets**.

3. On the right page, click the **Change secret tasks** tab.

4. Click **+ Create**.

5. In the **Name** field, type the task name.

6. In the **Accounts** field, type one or more usernames for which you want to change the secrets.

7. In the **Assets** field, select one or more assets. The task changes secrets for all accounts under the selected assets.

8. In the **Nodes** field, select one or more nodes. The task changes secrets for all accounts under the selected nodes and their subnodes.

9. In the **Secret strategy** field, you can choose "Specific secret" to set it manually, or "Random generate" to generate it randomly.

10. In the **Secret type** field, you can choose either "Password" or "SSH key".

11. In the **Password** field, type a password. (Specific secret & Password)

12. In the **SSH key strategy** field, you can choose "Replace (Replace only keys pushed by JumpServer)" or "Empty and append SSH KEY". (SSH Key)

13. In the **Private key** field, paste your private key. (Specific secret & SSH key)

14. In the **Key password** field, type the private key password. (Specific secret & SSH key)

15. In the **Password rules** field, set password rules, including length, uppercase and lowercase letters, numbers, special characters, and excluded characters. (Random generate & Password)

16. In the **Parameters** field, configure secret change parameters.

> **Note**
>
> Parameters can be configured only when selecting a Host-type asset or a node containing Host-type assets.

17. In the **Periodic** field, check to enable scheduled execution.

18. In the **Check connection after change** field, check to verify the connection after the push task is completed.

19. In the **Active** field, check to enable the task.

20. In the **Description** field, type the task description.

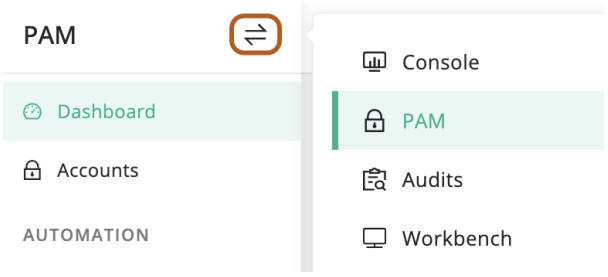
21. Click **Submit**.

Last updated on August 14, 2025

Create account risk detection task

Account risk detection checks password length, repeated passwords, and common weak passwords. Supports custom execution cycles for regular scanning of all accounts in JumpServer.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Risk detection**.

3. On the right page, click **Detection tasks** tab.

4. Click **+ Create**.

5. In the **Name** field, type the task name.

6. In the **Assets** field, select one or more assets. Detects accounts under the selected assets.

7. In the **Nodes** field, select one or more nodes. Detects accounts under assets in the selected nodes and their subnodes.

8. In the **Engines** field, select one or more check engines.

9. In the **Recipients** field, select one or more recipients. Sends the detection result after task completion.

10. In the **Periodic** field, check to enable scheduled execution.

11. In the **Active** field, check to enable the task.

12. In the **Description** field, type the task description.

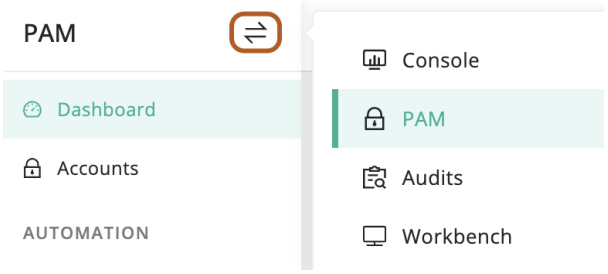
13. Click **Submit**.

Last updated on August 14, 2025

Create an application

Applications are used to allow external systems to call and retrieve accounts and passwords stored in JumpServer.

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Applications**.

3. On the right page, click the **Applications** tab.

4. Click **+ Create**.

5. In the **Name** field, type the application name.

6. In the **Logo** field, upload the application logo.

7. In the **Account** field, select one of the options: "All accounts", "Specific accounts", or "Filter by attribute".

8. In the **Access IP** field, type the IP address or range allowed to access the application.

9. In the **Active** field, check to enable the application.

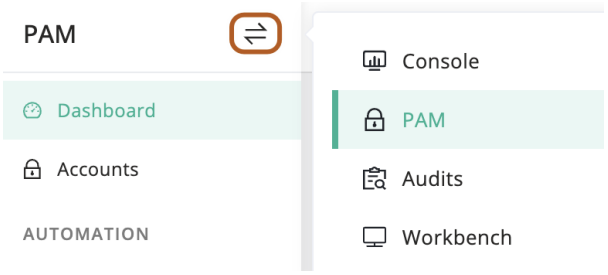
10. In the **Description** field, type the application description.

11. Click **Submit**.

Last updated on August 5, 2025

Application integration documentation

1. At the top-left of the page, select ⇌, then click **PAM**.



2. In the left menu, click **Applications**.

3. On the right page, click the **Documentation** tab. The API documentation provides examples in:

    - cURL
    - Python
    - Go
    - Java
    - Node.js

Last updated on August 12, 2025

General

Configuration guide

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **General**.

3. Modify the following configuration parameters.

4. Click **Submit**.

Configuration parameters

Site URL

`required`

This setting is used to generate the externally accessible JumpServer URL when required (for example, to create clickable links in notification messages).

Document URL

Custom documentation URL.

In the navigation bar, users can view it by clicking ? > Docs.

Support URL

Custom support URL.

In the navigation bar, users can view it by clicking ⓘ > Support.

Last updated on October 28, 2025

Organizations

Create an organization

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Organizations**.

3. Click **+ Create**.

4. Type the organization name and description.

5. Click **Submit**.

Rename global organization

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Organizations**.

3. Click **Setting**.

4. In the **Global org display** field, type the new name.

5. Click **Confirm**.

Last updated on October 29, 2025

System role

Create a system role

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click 👕 **Roles**.

3. On the right page, click the **System roles** tab.

4. Click **+ Create**.

5. Type the role name and description.

6. Click **Submit**.

Configure system role permissions

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click 👕 **Roles**.

3. On the right page, click the **System roles** tab.

4. Click the role name you want to configure to open the details page.

5. Click the **Basic** tab, and in the "Permission" section on the right side of the page, check or uncheck the corresponding permissions.

6. Click **Update**.

Last updated on October 29, 2025

Organization role

Create an organization role

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Roles**.

3. On the right page, click the **Organization roles** tab.

4. Click **+ Create**.

5. Type the role name and description.

6. Click **Submit**.

Configure organization role permissions

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Roles**.

3. On the right page, click the **Organization roles** tab.

4. Click the role name you want to configure to open the details page.

5. Click the **Basic** tab, and in the "Permission" section on the right side of the page, check or uncheck the corresponding permissions.

6. Click **Update**.

Last updated on October 29, 2025

Email service configuration guide

In JumpServer, the email server is an essential configuration and it is strongly recommended to enable and properly set it up. It is primarily used for communication between the system and users, including account security, notification alerts, and system warnings.

JumpServer supports configuring the email server in two ways: using the standard SMTP protocol or Microsoft Exchange Server.

Configuration guide

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click 🔔 **Notifications**.

3. On the right page, click **Email** tab.

4. Type the email configuration. About configuration parameters, see Configuration parameters.

5. Click **Submit**.

Configuration parameters

Service

- SMTP

  Standard SMTP protocol

- Microsoft Exchange Server

A mail server developed by Microsoft.

Host

`required`

Email server host address.

Port

`required`

(SMTP only) Email server port.

Account

Email server authentication account.

Password

Email server authentication account password.

Sender

The sender used to send emails. If not specified, the **Account** will be used by default.

Use ssl/tls

(SMTP only) Encrypts the communication between the email client and server to protect the email content and account information.

- None

  No encryption — plain text transmission (low security).

- SSL

  SSL (Secure Sockets Layer) is an older protocol for establishing secure connections.

- TLS

  TLS (Transport Layer Security) is an improved version of SSL, providing stronger security.

Template

Email templates are used to provide consistent content and formatting when sending emails.

General

General fields included in every email.

Subject prefix

`required`

Specifies a prefix to insert at the start of the email subject.

e.g., [JumpServer]

Creating User Content

The following fields are only used in emails sent upon successful user creation.

Subject

Email subject.

e.g., Create account successfully

Honorific

Email honorific.

e.g., Dear / Hello

Content

Email content.

You can use the variables `{name}`, `{username}`, and `{email}` to specify the corresponding user information.

Recipient

This is used only for receiving test emails. Only one email address can be entered at a time.

Test the email service

> **Note**
>
> Please submit the configuration information before testing.

1. Finish configuring the email service and **submit** the form.

2. In the **Recipient** field, type the email address to which you want to send a test email.

3. Click **Test connection**.

Last updated on August 22, 2025

Message template

Administrators can modify the corresponding notification templates as needed. The following types of message templates are currently supported for customization:

- Session sharing
- Different city login reminder
- OAuth binding reminder
- Create account successfully
- Reset password
- Reset password success
- Reset public key success
- Password is about expire
- Account is about expire
- Reset SSH Key
- Reset MFA
- User login reminder
- User login alert for asset

Edit a message templates

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click 🔔 **Notifications**.

3. On the right page, click **Msg template** tab.

4. In the **Name** field, select the message template to be edited.

   Below the field, click "ⓘHelp" to view the available variables for the selected template.

5. Click **Submit**.

Last updated on October 29, 2025

Message

Administrators can configure and enable SMS service. Currently, the following SMS providers are supported:

- Alibaba cloud
- Tencent cloud
- Huawei cloud
- CMPP v2.0
- Custom type
- Custom (File)

Enable SMS service

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click 🔔 **Notifications**.

3. On the right page, click **Message** tab.

4. In the **SMS** field, check the box to enable SMS service.

5. In the **Provider** field, select the SMS provider.

6. In the **Code length** field, set the length of the verification code. The default is 4.

7. In the **Provider** section, configure the parameters required by the selected SMS provider.

8. Click **Submit**.

Last updated on October 29, 2025

Announcement

Administrators can set announcements for all users, which users can view upon logging in.

Enable announcement

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Announcement** tab.

4. In the **Announcement** field, check the box to enable announcement.

5. For other information, refer to the configuration parameters.

6. Click **Submit**.

Configuration parameters

Subject

`required`

Announcement subject.

Content

`required`

Announcement content (Markdown format supported).

Date start

Announcement start date.

Date end

Announcement end date.

The announcement will only be displayed between the start and end dates.

More link

Optional link for more information. If provided, a "More" button will be displayed in the announcement for users to click and view additional details.

Last updated on October 29, 2025

Ticket

Enable ticket

1. In the right area of the top navigation bar, click .

2. In the left menu, click **Features**.

3. On the right page, click **Ticket** tab.

4. In the **Ticket** field, check the box to enable ticket.

5. For other information, refer to the configuration parameters.

6. Click **Submit**.

Configuration parameters

Approval without login

Whether administrators are allowed to approve tickets directly without logging in.

Period

Set the default validity period of authorization here when users apply for asset authorization.

Unit

Set the default unit of the authorization validity period here when users apply for asset authorization.

- day
- hour

Last updated on October 30, 2025

Job center

Administrators can globally enable the Adhoc feature for all users and configure the command blacklist in Adhoc.

Enable Adhoc

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Job center** tab.

4. In the **Adhoc command** field, check the box to enable Adhoc.

5. Click **Submit**.

> **Note**
>
> This setting controls not only the **Workbench > JOB CENTER > Job** feature but also the bulk command execution feature at the bottom of the **Luna (Web Terminal)** page.

Configuration command blacklist

Administrators can configure the command blacklist in Adhoc to prevent users from executing risky commands on assets.

> **Note**
>
> This command blacklist takes effect only in **Workbench > JOB CENTER > Adhoc**.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Job center** tab.

4. In the **Command blacklist** field, type the commands to be blacklisted, and press Enter after each command to confirm.

5. Click **Submit**.

Last updated on November 18, 2025

Account storage

Administrators can configure account storage for the system and store asset account credentials in an external system. The following account storage types are currently supported:

- HashiCorp Vault
- Microsoft Azure Key Vault
- Amazon Web Services Secrets Manager

> **Note**
> For security reasons, account storage can currently only be configured in the service configuration file (config.txt), and the JumpServer service must be restarted after configuration.

Enable account storage

Using HashiCorp Vault

Please refer to and modify the following configuration:

- VAULT_ENABLED
- VAULT_BACKEND
- VAULT_HCP_HOST
- VAULT_HCP_TOKEN
- VAULT_HCP_MOUNT_POINT

Using Microsoft Azure Key Vault

Please refer to and modify the following configuration:

- VAULT_ENABLED
- VAULT_BACKEND

- VAULT_AZURE_HOST
- VAULT_AZURE_CLIENT_ID
- VAULT_AZURE_CLIENT_SECRET
- VAULT_AZURE_TENANT_ID

Using Amazon Web Services Secrets Manager

Please refer to and modify the following configuration:

- VAULT_ENABLED
- VAULT_BACKEND
- VAULT_AWS_REGION_NAME
- VAULT_AWS_ACCESS_KEY_ID
- VAULT_AWS_ACCESS_SECRET_KEY

Set the maximum number of account secret records

Administrators can set the maximum number of account secret records stored in the external vault system to avoid excessive storage usage.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Account storage** tab.

4. In the **Record limit** field, type the maximum number of account secret records to be stored in the external vault system.

5. Click **Submit**.

Synchronize account secrets to external vault

After enabling account storage, administrators need to manually sync existing account secrets stored in JumpServer's local database to the external vault system.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Account storage** tab.

4. Click **Sync**.

> **Note**
>
> Account credentials can only be synchronized from the local database to the external account storage, reverse synchronization is not supported.

Last updated on October 30, 2025

Chat AI

Administrators can configure the Chat AI feature, allowing users to ask questions and chat through the AI assistant icon on the right side of the page.

Enable Chat AI

Two configuration methods are currently supported:

- `API`: Implemented by calling a general model.
- `Embed`: Implemented by directly embedding an iframe chat window.

Using GPT model

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.
3. On the right page, click **Chat AI** tab.
4. In the **Chat AI** field, check the box to enable Chat AI.
5. In the **Method** field, select "API".
6. In the **Types** field, select "GPT".
7. In the **Base URL** field, type the API base URL of the GPT model.
8. In the **API key** field, type the API key of the GPT model.

9. In the **Proxy** field, type the proxy address if a proxy is needed to access the GPT model API.

10. In the **GPT model** field, select the GPT model to be used. Available models:

    - gpt-4o-mini
    - gpt-4o
    - o3-mini
    - o1-mini
    - o1

11. Click **Submit**.

Using DeepSeek model

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.

3. On the right page, click **Chat AI** tab.

4. In the **Chat AI** field, check the box to enable Chat AI.

5. In the **Method** field, select "API".

6. In the **Types** field, select "DeepSeek".

7. In the **Base URL** field, type the API base URL of the DeepSeek model.

8. In the **API key** field, type the API key of the DeepSeek model.

9. In the **Proxy** field, type the proxy address if a proxy is needed to access the DeepSeek model API.

10. In the **DeepSeek model** field, select the DeepSeek model to be used. Available models:
    - DeepSeek-V3
    - DeepSeek-R1
11. Click **Submit**.

Using embed method

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Features**.
3. On the right page, click **Chat AI** tab.
4. In the **Chat AI** field, check the box to enable Chat AI.
5. In the **Method** field, select "Embed".
6. In the **Base URL** field, type the iframe URL of the chat window.
7. Click **Submit**.

Last updated on October 30, 2025

Basic settings

This topic describes some basic authentication-related configurations.

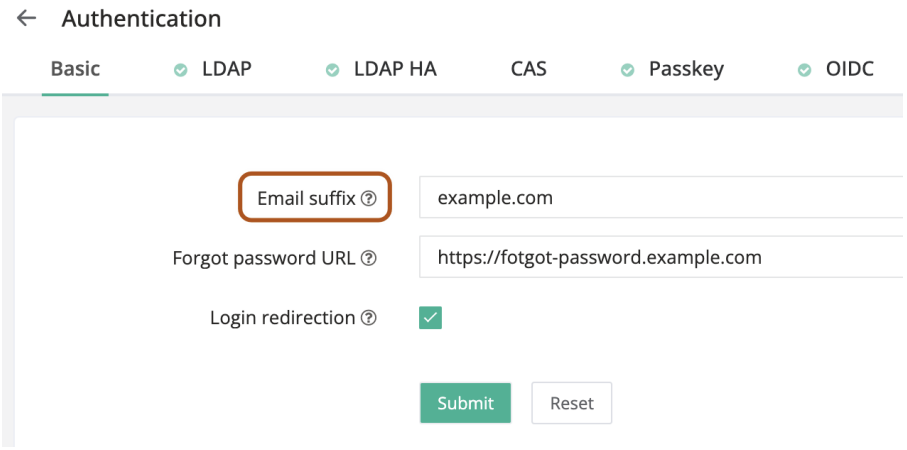
Email suffix

If the user from the third-party authentication does not have an email field configured, the email suffix is used to automatically generate the user email address by combining the username with the suffix.

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Basic**.

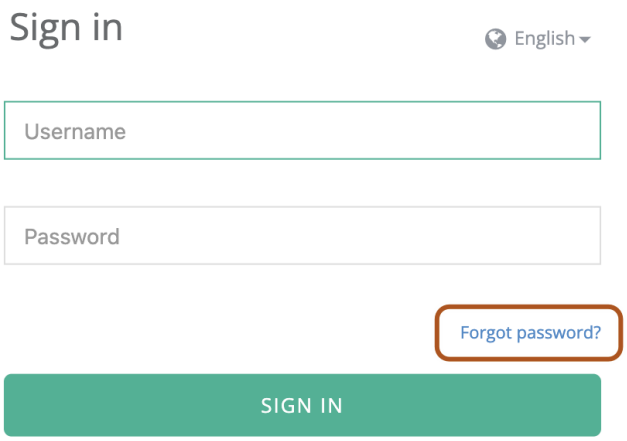
3. In the **Email suffix** field, type the email suffix, such as "example.com".



4. Click **Submit**.

Forgot password URL

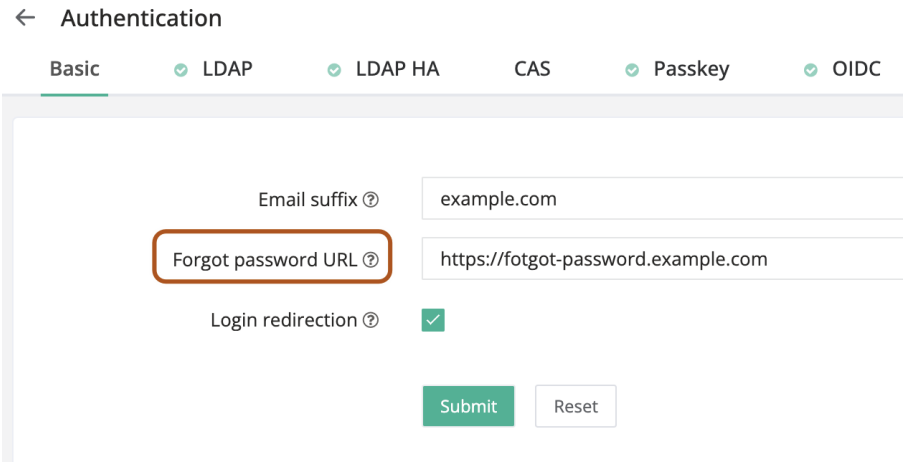
When the user clicks the `Forgot password?` on the login page, they will be redirected to "Forgot password URL".



1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Basic**.

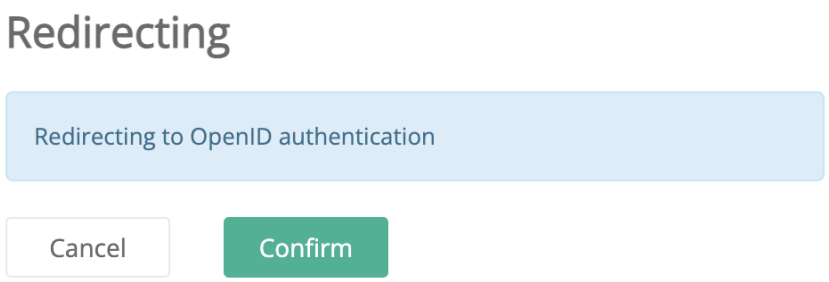
3. In the **Forgot password URL** field, type the URL for the forgot password link, such as "https://forgot-password.example.com".



4. Click **Submit**.

Login redirection

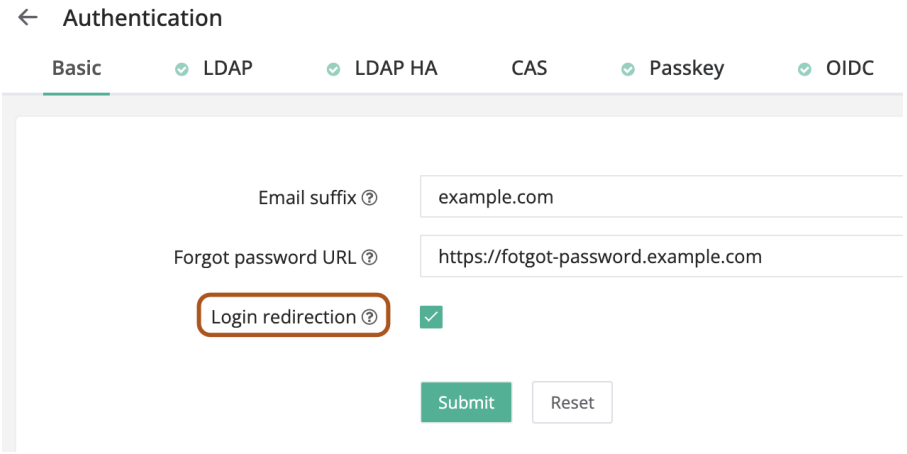
When an unauthenticated user accesses JumpServer, if checked, they will be prompted to either **Cancel** and return to the default login page or **Confirm** to proceed with third-party authentication. If unchecked, they will be directly redirected to the third-party authentication page.



1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Basic**.

3. In the **Login redirection** field, check to enable user login redirection.



4. Click **Submit**.

Last updated on August 12, 2025

Integrate AD/LDAP authentication

About LDAP

Lightweight Directory Access Protocol (LDAP) is an open protocol used for accessing and managing distributed directory information. It is commonly used for centralized authentication and directory services, such as storing user accounts, permissions, and organizational structure information. LDAP is widely applied in enterprise identity management, single sign-on (SSO), and access control systems.

Distinguished Name (DN) is unique identifier for each entry in an LDAP directory, similar to a file path in a filesystem, such as "cn=admin,ou=Users,dc=example,dc=com".

Organizational Unit (OU) is used to organize and manage objects in an LDAP directory, similar to folders in a file system. For example, an organization may have multiple OUs "ou=HR" and "ou=IT", to distinguish users and resources of different departments.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > LDAP**.

3. In the **LDAP** field, check to enable LDAP authentication.

4. In the **Server** field, type the LDAP server URI, such as "ldap://example.com:389" and "ldaps://example.com:636".

> **Tip**

> To configure LDAP TLS certificates, you can upload the files "ldap_ca.pem, ldap_cert.pem, ldap_cert.key" to the directory "/data/jumpserver/core/data/certs", then restart the service.

5. In the **Bind DN** field, type a user DN with at least query permissions, which will be used to query and filter users, such as "cn=admin,dc=example,dc=com".

6. In the **Password** field, type the password for the "Bind DN" user.

7. In the **Search OU** field, type the search OU to specify where to start searching for users, use `|` to separate multiple values, such as "ou=users,dc=example,dc=com | ou=tech,dc=example,dc=com".

8. In the **Search filter** field, type the filter expression to search for LDAP users. By default, the expression is "(cn=%(user)s)", where "%(user)s" is the placeholder syntax in Python. During filtering, it is replaced with `*`, resulting in "(cn=*)", which searches for all users. You can also replace "cn" with the actual username field, such as "uid" or "sAMAccountName".

9. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, is_active, groups, phone, comment), while the value corresponds to the LDAP user attribute name.

LDAP User Attribute Example

```
{
  "name": "cn",
  "email": "mail",
  "username": "cn",
  "is_active": "useraccountcontrol",
  "groups": "memberOf"
}
```

10. In the **Connect timeout (s)** field, type the LDAP connection timeout in seconds.

11. In the **Search paged size (piece)** field, type the page size for searching users.

12. In the **User DN cache timeout (s)** field, type the cache duration for user DN in seconds to improve login authentication speed. Submit the form to clear the cache if the user DN is changed, otherwise, authentication will fail.

13. Click **Submit**.

Test LDAP connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP**.

3. Scroll to the bottom of the page.

4. Click **Test connection**.

Test LDAP user login

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP**.

3. Completed and tested LDAP configuration successfully.

4. Scroll to the bottom of the page.

5. Click **Test login**.

6. In the pop-up window, type the username and password for LDAP user.

7. Click **Confirm**.

Import LDAP users

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP**.

3. Completed and tested LDAP configuration successfully.

4. Scroll to the bottom of the page.

5. Click **User import**.

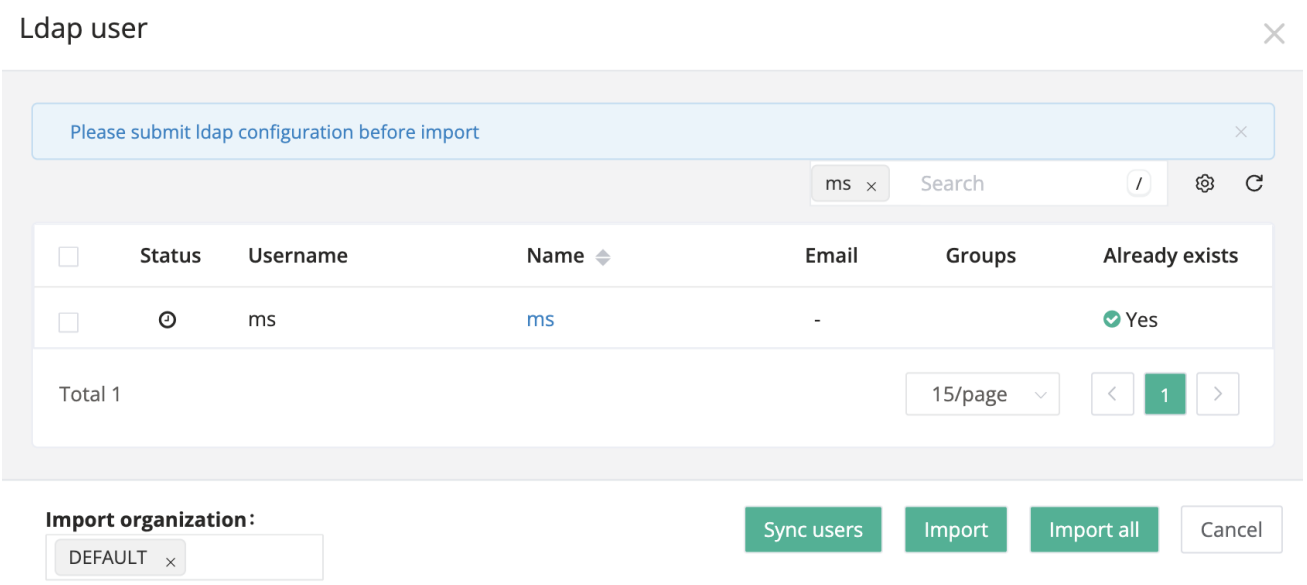
6. In the pop-up window, you can import LDAP users in the following ways.

    1. Click **Sync Users** to sync LDAP users to the table.

    2. 👑 In the **Import organization** field, select one or more organizations to import.

    3. Check the users you want to import, click **Import** to proceed.

    4. Alternatively, you can click **Import all** to import all users.



Set up LDAP user sync

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP**.

3. Completed and tested LDAP configuration successfully.

4. Scroll to the bottom of the page.

5. Click **Sync settings**.

6. In the pop-up window, type the following information to configure.

    1. 👑 In the **Organization** field, Select one or more organizations to sync.

    2. In the **Periodic** field, check to enable periodic sync.

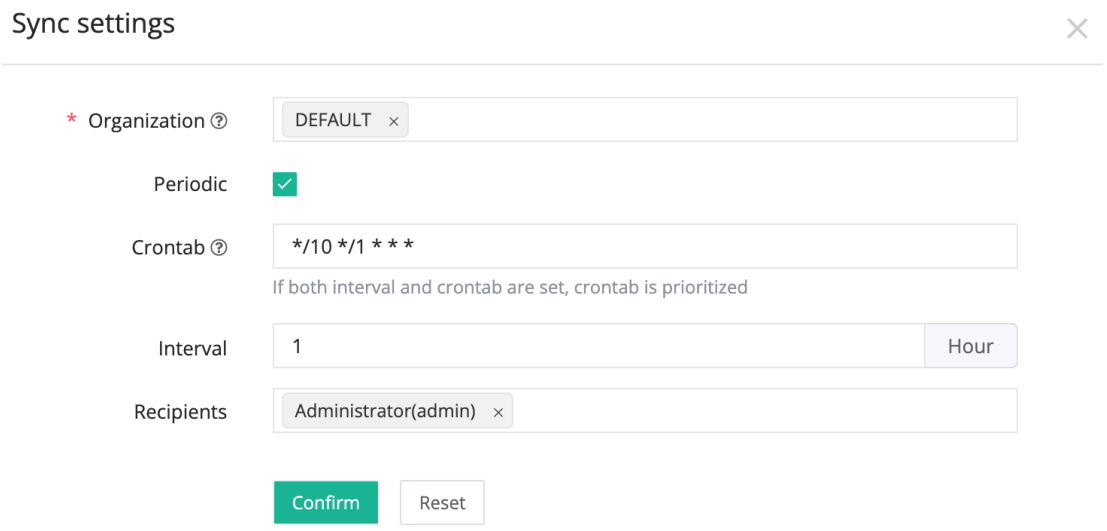
    3. In the **Crontab** field, type the crontab expression. If empty, "Interval" will be used.

4. In the **Interval** field, type the sync interval in hours.

   However, if "Crontab" has a value, "Crontab" will take priority.

5. In the **Recipients** fields, select one or more users to receive the sync result.

6. Click **Confirm**.



Last updated on October 31, 2025

Integrate CAS authentication

About CAS

Central Authentication Service (CAS) is a Single Sign-On (SSO) protocol designed to provide centralized authentication for multiple applications. Developed by Yale University, CAS allows users to access multiple protected services with a single login, eliminating the need to re-enter credentials. It implements authentication through a "ticket" mechanism and supports various identity providers, such as databases, LDAP, and OAuth.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > CAS**.

3. In the **CAS** field, check to enable CAS authentication.

4. In the **Server** field, type the CAS server URI, such as "https://example.com/cas".

5. In the **Proxy server** field, type the CAS proxy server URI if behind a proxy. For example, if the host listens on "http://foo.bar:8080" but requests use "https://foo.bar:8443", enter "https://foo.bar:8443", For more information, see Django CAS configuration.

6. In the **Version** field, type the CAS protocol version: 1, 2, 3, or CAS_2_SAML_1_0.

   The default is "3".

7. In the **User attribute** field, type the user attribute mapping. The key represents the CAS user attribute name, while the value corresponds to the JumpServer user attribute name (available options: name, username, email, groups, phone, comment).

CAS User Attribute Example

```
{
  "cas:user": "username",
  "cas:fullname": "name",
  "cas:mail": "email",
}
```

8. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

9. In the **Create user** field, when checked, a user will be created upon successful authentication.

> **Warning**
>
> When unchecked and the user does not exist, authentication will fail.

10. In the **Logout completely** field, when checked, logging out will also log the user out from the CAS service.

11. Click **Submit**.

JumpServer CAS URLs

Login URL

```
https://jumpserver.example.com/core/auth/cas/login/
```

Login Success Callback URL

```
https://jumpserver.example.com/core/auth/cas/callback/
```

Logout URL

```
https://jumpserver.example.com/core/auth/cas/logout/
```

Last updated on April 30, 2025

Integrate Passkey authentication

About Passkey

Passkey is a passwordless authentication technology based on public-key cryptography. It replaces traditional passwords to enhance security and user experience. Passkey is supported by the FIDO2 standard (including WebAuthn and CTAP) and allows users to authenticate using biometrics (fingerprint or facial recognition), a PIN, or a security key without entering a password.

Fast Identity Online (FIDO) is an open standard designed to provide a more secure, passwordless authentication method. It is developed by the FIDO Alliance and primarily includes FIDO UAF (Universal Authentication Framework) and FIDO2 (which consists of the WebAuthn and CTAP protocols).

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Passkey**.

3. In the **Passkey** field, check to enable Passkey authentication.

4. In the **FIDO server ID** field, type the full domain name of JumpServer, such as "jumpserver.example.com". If there are multiple domains, separate them with commas.

> **Tip**
>
> If not set, it defaults to the request host and matches domains in `DOMAINS` from "config.txt" file.

5. In the **FIDO server name** field, type the server name.

The default is "JumpServer".

6. Click **Submit**.

Last updated on April 30, 2025

Integrate AD/LDAP HA authentication

About LDAP HA

LDAP High Availability (LDAP HA) ensures the LDAP service remains operational during failures through specific configurations and technical measures. This improves the availability and reliability of directory services, ensuring that directory information within an organization is continuously accessible.

In JumpServer, the integration of LDAP HA typically ensures that if the primary LDAP server fails, the system can automatically switch to a backup LDAP HA server, ensuring the continuity of authentication services. This way, even if an LDAP server experiences issues, JumpServer can continue processing user authentication requests without causing downtime or service interruptions.

> **Tip**
>
> Configure LDAP before setting up LDAP HA. See Integrate LDAP guide

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP HA**.

3. In the **LDAP HA** field, check to enable LDAP HA authentication.

4. In the **Server** field, type the LDAP HA server URI, such as "ldap://example.com:389" and "ldaps://example.com:636".

> **Note**

> To configure LDAP HA TLS certificates, you can upload the files "ldap_ha_ca.pem, ldap_ha_cert.pem, ldap_ha_cert.key" to the directory "/data/jumpserver/core/data/certs", then restart the service.

5. In the **Bind DN** field, type a user DN with at least query permissions, which will be used to query and filter users, such as "cn=admin,dc=example,dc=com".

6. In the **Password** field, type the password for the "Bind DN" user.

7. In the **Search OU** field, type the search OU to specify where to start searching for users, use `|` to separate multiple values, such as "ou=users,dc=example,dc=com | ou=tech,dc=example,dc=com".

8. In the **Search filter** field, type the filter expression to search for LDAP HA users. By default, the expression is "(cn=%(user)s)", where "%(user)s" is the placeholder syntax in Python. During filtering, it is replaced with `*`, resulting in "(cn=*)", which searches for all users. You can also replace "cn" with the actual username field, such as "uid" or "sAMAccountName".

9. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, is_active, groups, phone, comment), while the value corresponds to the LDAP HA user attribute name.

LDAP HA User Attribute Example

```
{
  "name": "cn",
  "email": "mail",
  "username": "cn",
  "is_active": "useraccountcontrol",
  "groups": "memberOf"
}
```

10. In the **Connect timeout (s)** field, type the LDAP HA connection timeout in seconds.

11. In the **Search paged size (piece)** field, type the page size for searching users.

12. In the **User DN cache timeout (s)** field, type the cache duration for user DN in seconds to improve login authentication speed. Submit the form to clear the cache if the user DN is changed, otherwise, authentication will fail.

13. Click **Submit**.

Test LDAP HA connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP HA**.

3. Scroll to the bottom of the page.

4. Click **Test connection**.

Test LDAP HA user login

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP HA**.

3. Completed and tested LDAP HA configuration successfully.

4. Scroll to the bottom of the page.

5. Click **Test login**.

6. In the pop-up window, type the username and password for LDAP HA user.

7. Click **Confirm**.

Import LDAP HA users

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **LDAP HA**.

3. Completed and tested LDAP HA configuration successfully.

4. Scroll to the bottom of the page.

5. Click **User import**.

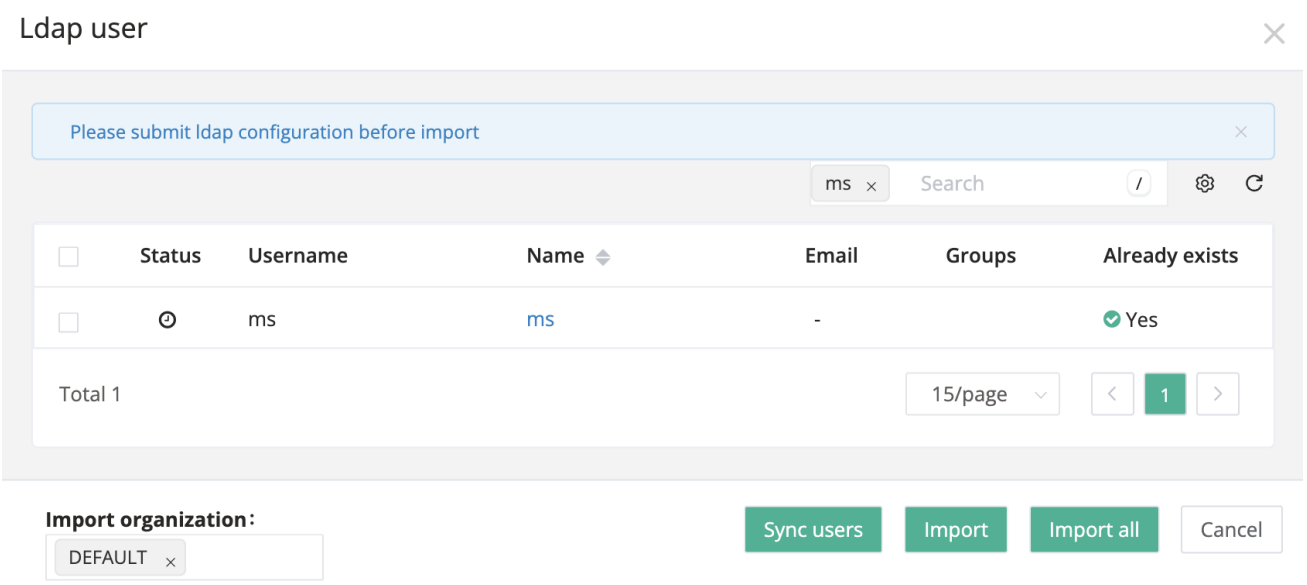
6. In the pop-up window, you can import LDAP HA users in the following ways.

    1. Click **Sync Users** to sync LDAP HA users to the table.

    2. In the **Import organization** field, select one or more organizations to import.

    3. Check the users you want to import, click **Import** to proceed.

    4. Alternatively, you can click **Import all** to import all users.



Set up LDAP HA user sync

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > LDAP HA**.

3. Completed and tested LDAP HA configuration successfully.

4. Scroll to the bottom of the page.

5. Click **Sync settings**.

6. In the pop-up window, type the following information to configure.

    1. In the **Organization** field, Select one or more organizations to sync.

    2. In the **Periodic** field, check to enable periodic sync.

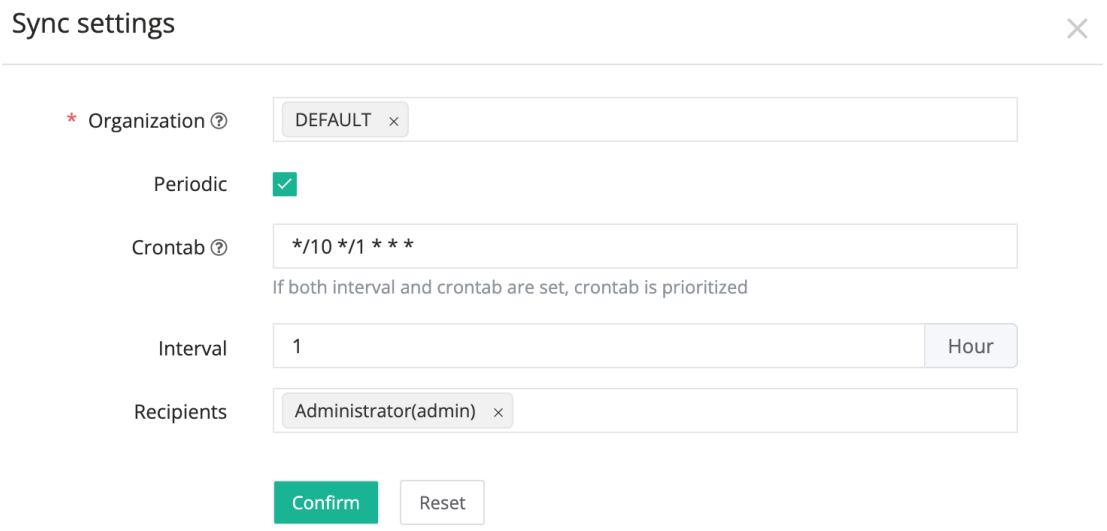
    3. In the **Crontab** field, type the crontab expression. If empty, "Interval" will be used.

4. In the **Interval** field, type the sync interval in hours.

   However, if "Crontab" has a value, "Crontab" will take priority.

5. In the **Recipients** fields, select one or more users to receive the sync result.

6. Click **Confirm**.



Last updated on October 31, 2025

Integrate OIDC authentication

About OIDC

OpenID Connect (OIDC) is an identity authentication protocol based on "OAuth 2.0". It allows applications to verify a user's identity through an "authorization server" and obtain basic user information, such as "username" and "email". It adds an identity layer on top of OAuth 2.0, using an "ID Token" to transmit user identity information, and is widely used for Single Sign-On (SSO) and identity authentication systems.

Relying Party (RP) is an application or client that uses authentication services and relies on the OpenID provider to authenticate the user and provide identity information.

OpenID Provider (OP) is the server responsible for verifying the user's identity and providing identity information to the RP.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > OIDC**.

3. In the **OIDC** field, check to enable OIDC authentication.

4. In the **Base site URL** field, type the full domain name of JumpServer, such as "https://jumsperver.example.com/", which is used to construct the callback URL.

5. In the **Client id** field, type the client id provided by the OIDC server.

6. In the **Client secret** field, type the client secret provided by the OIDC server.

7. In the **Request method** field, select a method to obtain a token.

    - `Client Secret Basic`: Use the POST method to obtain the token, with the client ID and client secret included in the request headers.
    - `Client Secret Post`: Use the POST method to obtain a token, with client ID and client secret included as "raw data" in the request body.

8. In the **Use keycloak** field, check to use the Keycloak configuration, or uncheck to use the native OIDC configuration.

    Use Keycloak | **Use Native OIDC**

    1. In the **Server** field, type the Keycloak server URI, such as "https://keycloak.example.com".

    2. In the **Realm name** field, type the Keycloak realm name, such as "JumpServer".

9. In the **Always update user** field, when checked, after OIDC user authentication, user information (only includes: name, username, email, phone, comment) will be updated each time, "groups" are only synchronized when the user is created.

10. In the **Ignore SSL verification** field, when checked, SSL certificate verification is ignored when sending requests to the OP.

11. In the **Share session** field, when checked, the session will be logged out simultaneously when a user logs out from other applications.

12. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, groups, phone, comment), while the value corresponds to the OIDC user attribute name.

OIDC User Attribute Example

```
{
  "name": "name",
  "username": "preferred_username",
  "email": "email",
  "groups": "groups"
}
```

13. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

14. Click **Submit**.

JumpServer OIDC URLs

Login URL

```
https://jumpserver.example.com/core/auth/openid/login/
```

Login Success Callback URL

```
https://jumpserver.example.com/core/auth/openid/callback/
```

Logout URL

```
https://jumpserver.example.com/core/auth/openid/logout/
```

Last updated on August 15, 2025

Integrate SAML2 authentication

About SAML2

Security Assertion Markup Language 2.0 (SAML2) is an open standard for exchanging authentication and authorization data between parties, particularly between an Identity Provider and a Service Provider. It allows users to authenticate once with the IdP and access multiple services (SPs) without needing to re-enter credentials.

Identity Provider (IdP) is a system that authenticates users and provides their identity information to service providers.

Service Provider (SP) is a system or application that relies on an IdP to authenticate users and grant access to its services based on the user identity. In this case, JumpServer acts only as the SP.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > SAML2**.

3. In the **SAML2** field, check to enable SAML2 authentication.

4. In the **SP private key** field, upload the SP private key file. It is used to sign SAML requests, decrypt encrypted SAML responses from the IdP, and ensure data integrity.

5. In the **SP cert** field, upload the SP certificate file. It is generated from the SP private key and provided to the IdP to verify signed requests from the SP. Additionally, it encrypts SAML response data to ensure secure transmission.

> **Note**

The SP private key and SP certificate work together to ensure secure communication and data protection in SAML2 authentication. In simple terms, SP private key handles signing and decryption, while the SP certificate handles verification and encryption.

6. In the **IDP metadata URL** field, type the IdP metadata URL, such as "https://saml2.example.com/realms/JumpServer/protocol/saml/descriptor".

7. In the **IDP metadata XML** field, you can manually type the IdP Metadata XML. In practice, you only need to provide either the "IDP metadata URL" or the "IDP metadata XML". If both are present, the "IDP metadata URL" takes precedence.

8. In the **SP advanced settings** field, type the information you want to configure. We will generate SP Metadata based on this configuration for IdP use. For more information, see SP advanced settings.

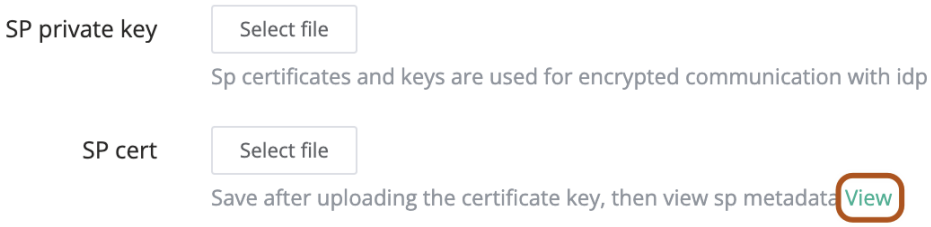
SAML2 SP Advanced Settings Example

```
{
  "organization": {
    "en": {
      "name": "JumpServer",
      "displayname": "JumpServer",
      "url": "https://jumpserver.com/"
    }
  },
  "strict": true,
  "security": {}
}
```

Note

SP Metadata is used to provide essential configuration information about the service provider, including entity ID, endpoint URLs, public certificates, and supported bindings, to facilitate secure communication with the identity provider in SAML authentication.

You can click *View* in the help information below the "SP cert" field to see the SP metadata.



9. In the **User attribute** field, type the user attribute mapping. The key represents the SAML2 user attribute name, while the value corresponds to the JumpServer user attribute name (available options: name, username, email, groups, phone, comment).

SAML2 User Attribute Example

```
{
  "uid": "username",
  "email": "email",
  "member": "groups"
}
```

10. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

11. In the **Always update user** field, when checked, after SAML2 user authentication, user information (only includes: name, username, email, phone, comment) will be updated each time, "groups" are only synchronized when the user is created.

12. In the **Logout completely** field, when checked, logging out will also log the user out from the SAML2 service.

13. Click **Submit**.

JumpServer SAML2 URLs

Login URL

```
https://jumpserver.example.com/core/auth/saml2/login/
```

Login Success Callback URL

```
https://jumpserver.example.com/core/auth/saml2/callback/
```

Logout URL

```
https://jumpserver.example.com/core/auth/saml2/logout/
```

SP Metadata URL

```
https://jumpserver.example.com/core/auth/saml2/metadata/
```

Last updated on August 8, 2025

Integrate OAuth2 authentication

About OAuth2

Open Authorization 2.0 (OAuth2) is an open authorization protocol that allows third-party applications to access user resources stored on other service providers (such as Google, Facebook, GitHub, etc.) without exposing the user's password. OAuth2 enables users to grant third-party applications specific resource permissions without sharing their login credentials.

How to configure

1. In the right area of the top navigation bar, click ⚙.

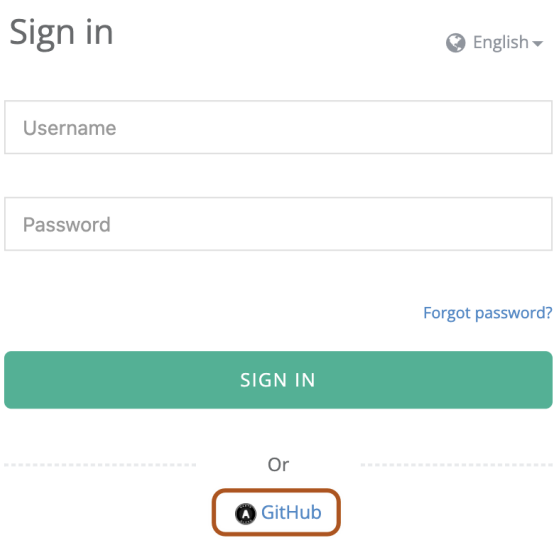
2. Navigate to the **System settings > Authentication > OAuth2**.

3. In the **OAuth2** field, check to enable OAuth2 authentication.

4. In the **Service provider** field, type the OAuth2 service provider name, such as GitHub, Google, Facebook, etc.

5. In the **Logo** field, upload the OAuth2 service provider logo, recommended to use a size of *64px * 64px*.

   The Service provider and logo will be displayed on the login page.



6. In the **Client ID** field, type the client ID provided by the OAuth2 service provider.

7. In the **Client secret** field, type the client secret provided by the OAuth2 service provider.

8. In the **Request method** field, select a method to obtain a token.

   - `GET`: Use the GET method to obtain the token, with the client ID and client secret included in the request headers.
   - `POST-DATA`: Use the POST method to obtain a token, with client ID and client secret included as "raw data" in the request body.
   - `POST-JSON`: Use the POST method to obtain a token, with client ID and client secret included as "JSON data" in the request body.

9. In the **Scope** field, defines the range of user information that the client requests access to in an authorization request. Multiple pieces of information are separated by spaces, such as "user user:email user:login".

10. In the **Authorization endpoint** field, type the OAuth2 authorization endpoint, such as "https://github.com/login/oauth/authorize".

11. In the **Token endpoint** field, type the OAuth2 token endpoint, such as "https://github.com/login/oauth/access_token".

12. In the **Userinfo endpoint** field, type the OAuth2 userinfo endpoint, such as "https://api.github.com/user".

13. In the **End session endpoint** field, type the OAuth2 end session endpoint, such as "https://github.com/logout", when the user logs out, this endpoint will be called.

14. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, groups, phone, comment), while the value corresponds to the OAuth2 user attribute name.

    OAuth2 User Attribute Example

    ```
    {
      "name": "user",
      "username": "name",
      "email": "user:email"
    }
    ```

15. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

16. In the **Always update user** field, when checked, after OAuth2 user authentication, user information (only includes: name, username, email, phone, comment) will be updated each time, "groups" are only synchronized when the user is created.

17. In the **Logout completely** field, when checked, the user will be logged out from the OAuth2 service by calling the "End session endpoint" upon logging out.

18. Click **Submit**.

JumpServer OAuth2 URLs

Login URL

```
https://jumpserver.example.com/core/auth/oauth2/login/
```

Login Success Callback URL

```
https://jumpserver.example.com/core/auth/oauth2/callback/
```

Logout URL

```
https://jumpserver.example.com/core/auth/oauth2/logout/
```

Last updated on August 15, 2025

Integrate WeCom authentication

About WeCom

WeCom authentication is an identity verification method based on WeCom (Enterprise WeChat), supporting OAuth 2.0 authorization, QR code login, and enterprise identity binding, enabling secure and convenient enterprise user login and management.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **WeCom**.

3. In the **WeCom** field, check to enable WeCom authentication.

4. In the **Corporation ID** field, type the WeCom corporation ID. Uniquely identifies the enterprise in WeCom, and all API requests must include this ID.

5. In the **App agent ID** field, type the WeCom app agent ID. Used to identify a specific application in WeCom, with each application having a unique Agent ID.

6. In the **App secret** field, type the WeCom app secret. Used to authenticate the application and obtain an access token for calling the WeCom API.

7. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, phone, comment), while the value corresponds to the WeCom user attribute name.

WeCom User Attribute Example

```
{
  "name": "alias",
  "username": "userid",
  "email": "extattr.attrs[2].value"
}
```

8. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

9. Click **Submit**.

Test WeCom connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **WeCom**.

3. Scroll to the bottom of the page.

4. Click **Test**.

JumpServer WeCom URLs

QR Login URL

```
https://jumpserver.example.com/core/auth/wecom/qr/login/
```

QR Login Success Callback URL

```
https://jumpserver.example.com/core/auth/wecom/qr/login/callback/
```

OAuth Login URL

```
https://jumpserver.example.com/core/auth/wecom/oauth/login/
```

OAuth Login Success Callback URL

```
https://jumpserver.example.com/core/auth/wecom/oauth/login/callback/
```

Last updated on August 8, 2025

Integrate DingTalk authentication

About DingTalk

DingTalk authentication is an identity verification method based on DingTalk, supporting OAuth 2.0 authorization, QR code login, and enterprise identity binding, enabling secure and convenient enterprise user login and management.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **DingTalk**.

3. In the **DingTalk** field, check to enable DingTalk authentication.

4. In the **Agent ID** field, type the DingTalk agent ID, which uniquely identifies a micro-application within the enterprise and is primarily used for sending work notifications.

5. In the **App key** field, type the DingTalk app key, a unique identifier for the application, similar to a username for API access.

6. In the **App secret** field, type the DingTalk app secret, similar to a password for API access, used to obtain AccessToken for calling APIs.

7. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, phone, comment), while the value corresponds to the DingTalk user attribute name.

DingTalk User Attribute Example

```
{
  "name": "name",
  "username": "name",
  "email": "email"
}
```

8. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

9. Click **Submit**.

Test DingTalk connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **DingTalk**.

3. Scroll to the bottom of the page

4. Click **Test**.

JumpServer DingTalk URLs

QR Login URL

```
https://jumpserver.example.com/core/auth/dingtalk/qr/login/
```

QR Login Success Callback URL

```
https://jumpserver.example.com/core/auth/dingtalk/qr/login/callback/
```

OAuth Login URL

```
https://jumpserver.example.com/core/auth/dingtalk/oauth/login/
```

OAuth Login Success Callback URL

```
https://jumpserver.example.com/core/auth/dingtalk/oauth/login/callback/
```

Last updated on August 8, 2025

Integrate FeiShu authentication

About FeiShu

FeiShu authentication is an identity verification mechanism based on the FeiShu platform, allowing enterprises and third-party applications to authenticate and authorize users through FeiShu.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > FeiShu**.

3. In the **FeiShu** field, check to enable FeiShu authentication.

4. In the **App ID** field, type the FeiShu app ID, a unique identifier for the application.

5. In the **App secret** field, type the FeiShu app secret, used to obtain an access token for calling the FeiShu API.

6. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, phone, comment), while the value corresponds to the FeiShu user attribute name.

FeiShu User Attribute Example

```
{
  "name": "nickname",
  "username": "user_id",
  "email": "email"
}
```

7. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

8. Click **Submit**.

Test FeiShu connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > FeiShu**.

3. Scroll to the bottom of the page

4. Click **Test**.

JumpServer FeiShu URLs

QR Login URL

```
https://jumpserver.example.com/core/auth/feishu/qr/login/
```

QR Login Success Callback URL

```
https://jumpserver.example.com/core/auth/feishu/qr/login/callback/
```

Last updated on August 8, 2025

Integrate Lark authentication

About Lark

Lark authentication is an identity verification mechanism provided by Lark (the international version of Feishu), enabling enterprises and third-party applications to authenticate and authorize users through Lark.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Lark**.

3. In the **Lark** field, check to enable Lark authentication.

4. In the **App ID** field, type the Lark app ID, a unique identifier for the application.

5. In the **App secret** field, type the Lark app secret, used to obtain an access token for calling the Lark API.

6. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, phone, comment), while the value corresponds to the Lark user attribute name.

Lark User Attribute Example

```
{
  "name": "nickname",
  "username": "user_id",
  "email": "email"
}
```

7. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

8. Click **Submit**.

Test Lark connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > Lark**.

3. Scroll to the bottom of the page.

4. Click **Test**.

JumpServer Lark URLs

QR Login URL

```
https://jumpserver.example.com/core/auth/lark/qr/login/
```

QR Login Success Callback URL

```
https://jumpserver.example.com/core/auth/lark/qr/login/callback/
```

Last updated on August 8, 2025

Integrate Slack authentication

About Slack

Slack authentication is an identity verification mechanism based on the Slack platform, allowing users to log in to enterprise applications or third-party services using their Slack accounts for secure authentication and authorization.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings > Authentication > Slack**.

3. In the **Slack** field, check to enable Slack authentication.

4. In the **Client ID** field, type the Slack client ID, a unique identifier for your Slack application, used to identify the app during the OAuth 2.0 authorization process.

5. In the **Client secret** field, type the Slack client secret, a confidential string associated with your Slack application, used to authenticate the app during the OAuth 2.0 token exchange process.

6. In the **Client bot token** field, type the Slack client bot token, an access token granted to your Slack bot, allowing it to interact with the Slack workspace and perform tasks like sending messages or managing channels.

7. In the **User attribute** field, type the user attribute mapping. The key represents the JumpServer user attribute name (available options: name, username, email, phone, comment), while the value corresponds to the Slack user attribute name.

Slack User Attribute Example

```
{
  "name": "real_name",
  "username": "name",
  "email": "profile.email"
}
```

8. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

9. Click **Submit**.

Test Slack connection

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Slack**.

3. Scroll to the bottom of the page.

4. Click **Test**.

JumpServer Slack URLs

QR Login URL

```
https://jumpserver.example.com/core/auth/slack/qr/login/
```

QR Login Success Callback URL

```
https://jumpserver.example.com/core/auth/slack/qr/login/callback/
```

Last updated on August 8, 2025

Integrate RADIUS authentication

About RADIUS

Remote authentication Dial-In User Service (RADIUS) is a remote authentication mechanism based on the RADIUS protocol, primarily used for network access control. It provides Authentication, Authorization, and Accounting (AAA) functionalities.

How to configure

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **Authentication** > **Radius**.

3. In the **Radius** field, check to enable RADIUS authentication.

4. In the **Host** field, type the RADIUS server IP address or domain name, such as "172.16.10.180".

5. In the **Port** field, type the RADIUS server port number. The default is "1812".

6. In the **Secret** field, type the shared secret key between the JumpServer and the RADIUS server. It functions like a password, encrypting sensitive information in RADIUS requests and responses to ensure secure communication.

7. Optionally, in the **OTP in RADIUS** field, check to enable RADIUS as the MFA backend. For more information, see Enable RADIUS MFA backend.

8. In the **Organization** field, after authentication and creation, the user will be added to the selected organization.

9. Click **Submit**.

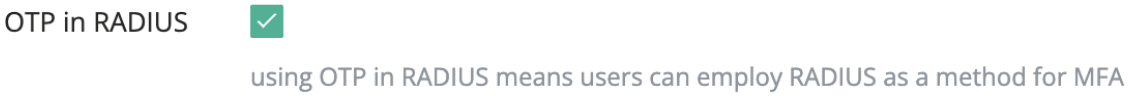
Enable RADIUS MFA backend

This subsection describes how to configure RADIUS authentication as one of the MFA backends.

1. Configure RADIUS authentication by following the Integrate RADIUS authentication guide.

2. In the **OTP in RADIUS** field, check to enable RADIUS as the MFA backend.

   When a user's MFA is enabled, they can choose RADIUS authentication type during login.



3. Click **Submit**.

Last updated on August 8, 2025

Object storage

JumpServer allows administrators to configure object storage for saving asset session recordings.

The following object storage types are currently supported:

- Built-in types:
    - Local (stores recordings locally)
    - Null (does not store recordings)
- Cloud or external storage types:
    - Amazon S3
    - Ceph
    - OpenStack Swift
    - Alibaba Cloud OSS
    - Microsoft Azure Blob Storage
    - Huawei Cloud OBS
    - Tencent Cloud COS
- Backup-only storage:
    - SFTP (used only for storing backup files, such as account backups)

Create an object storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Object storage** tab.

4. Click **+ Create**, and select the desired object storage type.

5. Fill in the required information for the selected object storage type.

6. Click **Submit**.

Set the default object storage

After setting a default storage, newly registered components will automatically use it. The object storage type of existing components will remain unchanged.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Object storage** tab.

4. Find the object storage you want to set as default.

5. In the Actions column, click the ··· icon, then click **Set as default**.

> **Note**
>
> SFTP storage cannot be set as the default object storage.

Test the object storage

You can test whether the configured object storage is working properly.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Object storage** tab.

4. Find the object storage you want to test.

5. In the Actions column, click the ··· icon, then click **Test**.

Edit an object storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Object storage** tab.

4. Find the object storage you want to edit.

5. In the Actions column, click **Edit**.

Delete an object storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Object storage** tab.

4. Find the object storage you want to delete.

5. In the Actions column, click the ··· icon, then click **Delete**.

Last updated on October 31, 2025

Command storage

JumpServer allows administrators to configure command storage for saving command logs generated during asset sessions.

The following command storage types are currently supported:

- Built-in types:
  - Local (stores command logs locally)
  - Null (does not store command logs)
- Cloud or external storage types:
  - Elasticsearch

Create a command storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Command storage** tab.

4. Click **+ Create**, and select the desired command storage type.

5. Fill in the required information for the selected command storage type.

6. Click **Submit**.

Set a default command storage

After setting a default storage, newly registered components will automatically use it. The command storage type of existing components will remain unchanged.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Command storage** tab.

4. Find the command storage you want to set as default.

5. In the Actions column, click the ··· icon, then click **Set as default**.

Test the command storage

You can test whether the configured command storage is working properly.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Command storage** tab.

4. Find the command storage you want to test.

5. In the Actions column, click the ··· icon, then click **Test**.

Edit a command storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Command storage** tab.

4. Find the command storage you want to edit.

5. In the Actions column, click **Edit**.

Delete a command storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Storage**.

3. On the right page, click **Command storage** tab.

4. Find the command storage you want to delete.

5. In the Actions column, click the ··· icon, then click **Delete**.

Last updated on October 31, 2025

General

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Basic** tab.

4. View and modify related configuration options.

5. Click **Submit**.

Configuration options

Registration

Configure whether components are allowed to register.

- `Auto`: (default) Allows component registration within 5 minutes after the service starts.
- `Enable`: Always allows component registration.
- `Disable`: Prevents component registration.

Client connection

Configure whether to allow connecting to the KoKo component via an SSH client.

When enabled, the SSH Client launch method will be displayed on the Luna page when users connect to assets.

Password

Configure whether to allow users to connect to the KoKo component using password authentication.

Public key

Configure whether to allow users to connect to the KoKo component using public key authentication.

If you have enabled a third-party authentication service, such as AD/LDAP, you should disable this option, otherwise, users will bypass the unified authentication system.

Asset sorting

Configure the default asset sorting field when users log in to the KoKo component to view assets.

- `Name`: (default) Sort assets by name in ascending order.
- `Address`: Sort assets by address in ascending order.

Asset page size

Configure the default number of assets displayed per page when users log in to the KoKo component to view assets.

- `Auto`: (default) Automatically adjust the number of assets displayed per page based on the screen size.
- `All`: Display all assets on a single page.
- `10`: Display 10 assets per page.
- `15`: Display 15 assets per page.
- `25`: Display 25 assets per page.
- `50`: Display 50 assets per page.

Razor

Configure whether to allow connecting to assets via the RDP protocol through Razor.

When enabled, the Luna page will display options to download the RDP file and connect to assets using an RDP client.

Magnus

Configure whether to allow connecting to databases via Magnus.

When enabled, the Luna page will display options to connect to assets using a database (DB) client.

Last updated on November 4, 2025

Components

For more information about JumpServer components, see About components.

Set the component's replay storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Components** tab.

4. Find the component whose replay storage you want to set.

5. In the Actions column, click **Edit**.

6. In the **Replay storage** field, select the desired object storage from the dropdown list.

7. Click **Submit**.

Set the component's command storage

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Components** tab.

4. Find the component whose command storage you want to set.

5. In the Actions column, click **Edit**.

6. In the **Command storage** field, select the desired command storage from the dropdown list.

7. Click **Submit**.

Delete offline components

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Components** tab.

4. Find the offline component you want to delete.

5. In the Actions column, click **Delete**.

6. In the confirmation dialog, click **OK** to delete the component.

Last updated on November 4, 2025

Monitoring

JumpServer provides a built-in monitoring page that allows administrators to monitor the real-time status of components. The page aggregates and displays status statistics for various components, including the number of components in normal, higher(high-load), serious(critical-load), and offline states, as well as the total number of active sessions for each component type.

Monitoring components

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Monitoring** tab.

Last updated on November 4, 2025

Endpoint

A service endpoint is the address (and port) through which users access the service. When users connect to assets, the system selects a service endpoint based on Endpoint rules and asset tags, and uses it as the access point to establish a connection, enabling distributed access to assets.

Create endpoint

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Endpoint** tab.

4. Click **+ Create**.

5. In the **Name** field, type a name for the endpoint.

6. In the **Host** field, type the domain name of the endpoint. The host address accessed when connecting to assets, if it is empty, the access address of the current browser will be used (the default endpoint does not allow modification of the host)

7. In the **Port** section, configure the correct service port.

8. Click **Submit**.

Last updated on November 4, 2025

Endpoint rules

Endpoint rules define how the system selects service endpoints based on rules when users connect to assets. By configuring endpoint rules, you can control and optimize access to assets, ensuring that users connect through the most appropriate endpoints based on predefined conditions.

For the server endpoint selection strategy, there are currently two options:

1. Specify the endpoint according to the endpoint rule (current page);
2. Choose the endpoint through asset tags, with the fixed tag name being "endpoint" and the value being the name of the endpoint.

The tag matching method is preferred for both methods, as the ip range may conflict, and the tag method exists as a supplement to the rules.

Create endpoint rule

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Components**.

3. On the right page, click **Endpoint rules** tab.

4. Click **+ Create**.

5. In the **Name** field, type a name for the endpoint rules.

6. In the **Priority** field, type the priority of the endpoint rules. The lower the value, the higher the priority.

7. In the **Address** field, type the IP address or IP segment of the asset to be matched by the endpoint rules.

8. In the **Endpoint** field, select the endpoint to be used when the asset matches the address.

9. Click **Submit**.

Last updated on November 4, 2025

RemoteApp

In JumpServer, **RemoteApp** is an application designed to run on a RemoteApp machine, providing users with remote access to specific software without needing a full remote desktop session. It features auto-fill functionality to enhance user experience by automating input tasks.

By supporting various connection protocols, RemoteApp offers users flexible options to connect to assets securely and efficiently. This makes it an ideal solution for accessing business-critical applications remotely, while simplifying management and improving security.

The built-in RemoteApps include "Chrome" and "DBeaver Community". For more RemoteApps, see App market.

Upload RemoteApp

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp** tab.

4. Click **App market** to open the App Store page and download the desired RemoteApp package (.zip).

5. Click **+ Upload** to upload the RemoteApp package (.zip) you have just downloaded.

Deploy RemoteApp

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp** tab.

4. Click the RemoteApp card to open the RemoteApp detail page.

5. In the RemoteApp detail page, click **RemoteApp machine** tab.

6. Find the RemoteApp machine you want to deploy, in the "Actions" column, click **Deploy**.

Delete RemoteApp

1. In the right area of the top navigation bar, click .

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp** tab.

4. Click RemoteApp card to open the RemoteApp detail page.

5. In the upper-right corner of the RemoteApp detail page, click the **Delete** button.

Last updated on June 17, 2025

RemoteApp machine

RemoteApp machine is a Windows host used to deploy RemoteApp services and install remote applications. Users can access and use the applications on this host remotely, enabling centralized management and remote usage.

Tinker is a tool provided by JumpServer for automating the deployment of RemoteApp services and publishing remote applications. When a user connects to a remote application, Tinker is also responsible for launching the application and performing auto-fill operations. Tinker is automatically installed by JumpServer during the deployment of the publishing machine.

Prerequisites

The RemoteApp machine must meet the following requirements:

- Running Windows Server 2019 Standard or Datacenter operating system.
- At least 4 CPU cores and 8 GB of RAM.
- OpenSSH or WinRM is installed and configured.
- Remote Desktop Services (RDS) license is installed and activated.
- Network access to JumpServer over HTTP/HTTPS is available.

Create a RemoteApp machine

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp machine** tab.

4. Above the table, click **+ Create**.

5. In the **Name** field, type RemoteApp machine's name.

6. In the **IP/Host** field, type the IP address or hostname.

7. In the **Protocols** field, set the protocol and port.

    - `rdp` is required for users to connect to the RemoteApp.
    - `ssh` requires the OpenSSH service to be installed on the machine.
    - `winrm` requires the WinRM service to be installed on the machine.

    You must select either ssh or winrm, as JumpServer uses them to manage the RemoteApp machine, including initial deployment and RemoteApp publishing.

8. In the **Accounts** field, add an account to manage the machine. It must meet the following requirements:

    - The account is a member of the Windows Administrators group.
    - Privileged is enabled.

9. Optionally, check **Using same account** to enable login with the same username.

    When the user connects to a RemoteApp , JumpServer will prioritize using a user with the same username to log in RemoteApp machine. This is especially useful when both JumpServer and the RemoteApp machine are integrated with the same AD/LDAP service.

    > **Important**
    >
    > For this feature to work, you need to set `CACHE_LOGIN_PASSWORD_ENABLED=true` in the `config.txt` file and restart the service.

10. Optionally, check **Auto create accounts** to generate two types of accounts automatically:

    - `js_` Private accounts use the prefix js_ followed by the user's username.
    - `jms_` Public accounts use the prefix jms_ followed by a random string.

When a user connects to a RemoteApp, the system first tries to log in to the RemoteApp machine using the `js_` account, which is private and unique to the user. If the RemoteApp on that machine doesn't support concurrent sessions for the same user, the system will instead use a random public `jms_` account.

11. Optionally, set **Accounts Create Amount** to specify the number of public `jms_` accounts.

12. In the **Core API** field, type the JumpServer IP address or hostname.

13. Optionally, check **Ignore certificate verification** to specify whether to ignore the certificate when Tinker accesses Core API.

14. Optionally, check **Existing RDS license** to use your own license. If unchecked, a 120-day trial license will be used. For more information, see RDS licensing documentation.

    1. In the **RDS license server** field, type the RDS license server address.

    2. In the **RDS licensing mode** field, choose the licensing mode.

    3. In the **RDS single session per user** field, set whether each user is allowed to have only one RDS session. If enabled, when a user connects a second session, the first session will be disconnected.

    4. In the **RDS max disconnection time (ms)** field, defines the maximum amount of time (in milliseconds) a disconnected session remains active.

    5. In the **RDS remote app logoff time limit (ms)** field, specifies how long the system waits before logging off a user after all RemoteApp programs are closed.

15. Optionally, in the **Zone** field, select only one zone.

16. Check **Active** to enable this RemoteApp machine.

17. Optionally, type a description for this machine.

18. Click **Submit** or **Save & Continue**.

Deploy the RemoteApp machine

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp machine** tab.

4. In the table, find the RemoteApp machine and click its name.

5. On the details page, click the **Deploy publishing machine** tab.

6. In the "Quick Update" card on the right, find "Initialization deployment" and click **Deploy**. This will start a task to initialize the deployment of the RemoteApp machine and publish all RemoteApp.

7. In the table on the left, you can view the deployment history and deployment logs.

Last updated on August 25, 2025

VirtualApp

In JumpServer, a **VirtualApp** is an application that includes an image address. When a user connects to an asset through a VirtualApp, Panda creates a corresponding VirtualApp container based on the image and establishes the connection through that container.

Panda, also called the **Application provider**, is a component of JumpServer. It is used to fetch VirtualApp images and manage containers, including creating, starting, stopping, and deleting containers.

Enable and configure VirtualApp

1. Enable VirtualApp

For details on how to enable the VirtualApp feature, see Enable virtual app.

2. Configure PANDA_HOST_IP

1. Log in to the Linux server using the "root" or another user with superuser privileges.
2. Edit the config file and type the current host IP.

```
vi  /opt/jumpserver/config/config.txt
```

```
PANDA_HOST_IP=Host-IP
```

3. Restart JumpServer.

```
jmsctl restart
```

Upload VirtualApp

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **RemoteApp** tab.

4. Click **App market** to open the App Store page and download the desired VirtualApp package (.zip).

5. On the right page, click **VirtualApp** tab.

6. Click **+ Upload** to upload the VirtualApp package (.zip) you have just downloaded.

Check VirtualApp status

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **Application providers** tab.

4. In the table, click the name of the application provider to open the details page.

5. On the details page, click **VirtualApp** tab.

6. You can view the image names and release status of all VirtualApps.

> **Tip**
>
> Panda retrieves the uploaded Virtual Apps every 5 minutes.

Check VirtualApp containers

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **RemoteApp**.

3. On the right page, click **Application providers** tab.

4. In the table, click the name of the application provider to open the details page.

5. On the details page, click **Container** tab.

6. You can view the created containers here when users connect to assets via Virtual Apps.

Last updated on October 31, 2025

Authentication security

This topic introduces configuration parameters for user authentication security.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Security**.

3. On the right page, click **Auth security** tab.

Basic

This section introduces the user login configurations.

Login CAPTCHA

`recommended`

Login CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) can effectively prevent brute-force attacks by malicious programs.

Once enabled, if a user fails to log in, any subsequent login attempts from the same IP within the next hour will require entering a CAPTCHA.

> **Note**
>
> Once enabled, the Login dynamic code and MFA in login page will be disabled.

Login dynamic code

Login dynamic code is concatenated with the user's password and sent together to the authentication service for verification.

For example, if the user's password is "passwd" and the dynamic code is "1234", the system will send "passwd1234" as the password to the backend authentication service during login.

This method is commonly used in scenarios such as RADIUS authentication.

> **Note**
>
> Once enabled, the Login CAPTCHA and MFA in login page will be disabled.

Auto disable threshold (day)

`required`

Default: `999` Min: `30` Max: `99999`

Automatically disabled users.

Users who have not logged in for more than the configured days will be automatically disabled.

For more information about enabling users, see Enable or disable users.

Suspicious login verification

Remote login alert.

If a user has not logged in from the city of their most recent login within the past 7 days, the system will send a remote login alert through the user's enabled message channels (e.g., in-site notifications, email, etc.).

MFA

This section introduces the MFA configurations.

Global MFA

Global MFA can be applied to all users at once, eliminating the need to configure it for each user individually, which simplifies administration.

- Not enabled

  Global MFA is disabled, but users can enable it from their profile page.

- All users

  Global MFA is enabled for all users and cannot be disabled by individual users.

- Only admin users

  Global MFA is enabled for admin users (including users with `System Admin` or `Organization Admin` roles) and cannot be disabled by them. Regular users can enable or disable it from their profile page.

Tip

If you have enabled global MFA but are unable to log in, you can run the following command to disable it.

```
docker exec -it jms_core bash
cd apps/
python manage.py shell
```

```
from settings.models import Setting
s = Setting.objects.get(name="SECURITY_MFA_AUTH")
s.value = 0
s.save()
```

MFA in login page

Effective only when "Global MFA" is enabled and "All users" is selected.

Once enabled, users will see the MFA code on the login page and can enter it together with their password for one-time verification.

If a user has not yet enabled MFA, they do not need to enter the MFA code on the login page. After the username and password are successfully verified, the system will guide the user through the MFA setup process.

> **Note**
>
> Once enabled, the Login CAPTCHA and Login dynamic code will be disabled.

MFA via email

Email can be used as an MFA authentication method. When users enable MFA and log in, they can choose to receive the MFA code via Email to complete verification.

> **Tip**
>
> Administrators must configure the Email service in advance. For more information, see Email service configuration guide.

Third-party login MFA

MFA can be enforced for users authenticated via third-party login methods. This applies mainly to redirection-based logins and QR code logins.

Authentication Method	Controlled by this setting
AD/LDAP	✗
CAS	✓
Passkey	✗
AD/LDAP HA	✗
OIDC	✓
SAML2	✓
OAuth2	✓
WeCom	✓
Dingtalk	✓
FeiShu	✓
Lark	✓
Slack	✓
RADIUS	✗

Users logging in through other authentication methods, like local users, can directly enable and use MFA.

MFA verify TTL

`required`

Default: `3600` (seconds)

When an administrator views an asset account's secret, the system requires MFA verification by default. This setting controls the validity period of the verification, with a default value of 3600 seconds. Within this period, subsequent secret views do not require repeated MFA verification.

For more information about disabling MFA verification when viewing account secrets, see SECURITY_VIEW_AUTH_NEED_MFA.

OTP issuer name

Default: `JumpServer`

When a user binds MFA, this field specifies the name of the service or application generating the OTP, helping the user distinguish codes from different services within their OTP app.

OTP valid window

`required`

Default: `2` Min: `0` Max: `10`

This setting controls the valid time window for one-time passwords (OTP). A new OTP is typically generated every 30 seconds, and to accommodate network delays or user input lag, the system allows OTPs from a few previous and subsequent time steps to remain valid.

If set to 2, the system accepts codes from the current, previous 2, and next 2 time steps.

If set to 0, only the current code is valid.

Last updated on November 4, 2025

Login restriction

This topic introduces configuration parameters for user login restrictions.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Security**.

3. On the right page, click **Login restriction** tab.

User

Within the **Login failure period (minute)**, if the number of consecutive failed login attempts exceeds **Login failures count**, the user will be locked and unable to log in.

Administrators can unlock the user from the User detail page, for more information, see Unlock user.

Login failures count

`required`

The number of consecutive failed login attempts by the user before the user is locked.

Login failure period (minute)

`required`

The time period within which the consecutive failed login attempts are counted.

IP

Within the **Login failure period (minute)**, if the number of consecutive failed login attempts exceeds **Login failures count**, the IP will be locked and no users will be able to log in from that IP.

Administrators can unlock the IP from the Locked ips section.

Login failures count

`required`

The number of consecutive failed login attempts from the IP before the IP is locked.

Login failure period (minute)

`required`

The time period within which the consecutive failed login attempts from the IP are counted.

Login IP whitelist

Set an IP whitelist. Users from these IPs will always be allowed to log in.

`*` represents matching all.

Login IP blacklist

Set an IP blacklist. Users from these IPs will always be denied login.

`*` represents matching all.

If you only want to allow specific IPs, set the "Login IP blacklist" to `*` and type the allowed IPs in the "Login IP whitelist".

Locked ips

View and manage the currently locked IPs.

Other

Only single device login

When enabled, a user can only be logged in from one device at a time. If the user logs in from another device, the previous session will be automatically logged out.

Only exist user login

When enabled, only existing users in the system are allowed to log in. Any login attempts with non-existing usernames will be denied.

Only from source login

When enabled, users can only authenticate and log in through the authentication service specified in their **Source** field.

Last updated on November 6, 2025

User password

This topic introduces configuration parameters for user password security.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Security**.

3. On the right page, click **User password** tab.

Basic

User password expiration (day)

The user password expiration period is calculated from the last password update. If the user does not change their password within this period, the password will expire, and the user will be unable to log in.

Within 5 days before the password expires, the system will automatically send a daily email reminder to prompt the user to update their password.

Recent password count

Administrators can configure that when users reset their passwords, the new password must not be the same as any of their recently used passwords.

User expired tokens record keep day

The system runs a scheduled task daily to delete expired connection tokens. Administrators can configure the number of days to retain them.

In "Profile Settings > Connection tokens", you can view and manage the connection tokens that are generated when connecting to assets.

Password rules

Leak password

Administrators can maintain a weak password set here.

The weak password set currently serves two purposes:

1. During asset account risk detection, any account whose password is included in the weak password set will be flagged as having a weak password.
2. When users reset their passwords, they are not allowed to use any password that is part of the weak password set.

Password complexity

Password complexity applies only to user passwords and does not include asset account passwords.

Minimum length (User)

Administrators can set a minimum password length for users.

Minimum length (Admin)

Administrators can set a minimum password length for administrators.

Uppercase

Administrators can configure whether user and administrator passwords must contain uppercase letters.

Lowercase

Administrators can configure whether user and administrator passwords must contain lowercase letters.

Digits

Administrators can configure whether user and administrator passwords must contain digits.

Special characters

Administrators can configure whether user and administrator passwords must contain special characters.

Last updated on November 5, 2025

Asset session

This topic introduces configuration parameters for asset session security.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Security**.

3. On the right page, click **Asset session** tab.

Basic

Session share

After session sharing is enabled, users can create share links within their active sessions and share them with other users. The invited users can then join the session. The following session types are currently supported for sharing:

- Web RDP
- Web VNC
- Web SSH

Session expire at browser closed

When enabled, the user session will expire when the user completely exits the browser.

Allow users to view asset session information

When enabled, the account selection pop-up will display the number of active sessions for the asset when users connect (RDP protocol only).

Max idle time (minute)

The maximum idle time for an asset session. If there is no activity within the specified time, the session will be automatically disconnected.

Max online time (hour)

The maximum online time for an asset session. Once the specified time is reached, the session will be automatically disconnected.

Watermark

Enable watermark

When the watermark feature is enabled, the watermark content will be displayed on the Lina (Console) page and in Luna (Asset session) asset sessions, and will also be retained in the session recordings.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Security**.

3. On the right page, click **Asset session** tab.

4. In the **Watermark** section, check the box to enable watermark.

5. Click **Submit**.

Configure watermark content

Session content

Configure the watermark content displayed in asset sessions.

You can use `${key}` to read built-in variables in watermark content. Built-in variables can be viewed by clicking "⑦Help" below the input box.

Console content

Configure the watermark content displayed in the console.

You can use `${key}` to read built-in variables in watermark content. Built-in variables can be viewed by clicking "⑦Help" below the input box.

Font color

Select the font color of the watermark.

Font size (px)

Set the font size of the watermark in pixels.

Height (px)

Set the height of the watermark in pixels.

Width (px)

Set the width of the watermark in pixels.

Rotate angle (degree)

Set the rotation angle of the watermark in degrees.

Last updated on November 6, 2025

Appearance

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Appearance**.

3. On the right-hand page, modify the appearance-related settings. For more details, refer to Configuration parameters.

4. Click **Submit**.

Configuration parameters

Login title

Customize the login title, which will be displayed as the page title when users log in to KoKo via the SSH terminal.

Theme

Change the system theme. The following themes are currently supported:

- Classic green (default)
- Chinese red
- Deep black
- Noble purple
- Technology blue

Wide logo on top

The logo will be displayed in the upper-left corner of the page (recommended size: 185 × 55 px).

Small logo without text

The logo will be displayed on the web terminal (Luna) page (recommended size: 82 × 82 px).

Website icon

The icon will be displayed in the browser tab (recommended size: 16 × 16 px).

Login image

The image will be displayed on the right side of the login page (recommended size: 492 × 472 px).

Footer content

Customize the footer content displayed at the bottom of the login page.

Restore default settings

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Appearance**.

3. On the right page, click the **Restore** button at the bottom of the page.

Last updated on November 6, 2025

Tools

You can use the following tools in JumpServer for network testing and troubleshooting:

- `ping`: Checks whether a host or network is reachable, used to verify network connectivity.
- `telnet`: Tests the connectivity of a specified host and port, commonly used to verify if a service port is open.
- `nmap`: Scans hosts and ports on the network for security and network analysis.
- `tcpdump`: Captures and analyzes network packets to help diagnose communication issues.
- `traceroute`: Traces the path of data packets to the target host to analyze network latency or routing problems.

Enable the tools feature in the Workbench

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Tools**.

3. In the **Tools in the workbench** fields, check to enable the tools feature in the Workbench.

4. Click **Submit**.

Last updated on November 6, 2025

Tasks

This page displays all system-related tasks, including their execution status and scheduled intervals.

Enable or disable tasks

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Tasks**.

3. On the right page, click **Tasks** tab.

4. Find the task you want to enable or disable, and click the switch button in the **Enable** column to enable or disable the task.

Monitor task status

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Tasks**.

3. On the right page, click **Tasks** tab.

4. Click **Monitoring**.

5. A new tab will open the Flower task monitoring page, where you can view the tasks running in each worker as well as the overall summary.

Last updated on November 6, 2025

Regular clean-up

This section introduces the regular clean-up tasks that can be configured in JumpServer.

1. In the right area of the top navigation bar, click ⚙.

2. In the left menu, click **Tasks**.

3. On the right page, click **Regular clean-up** tab.

4. Configure the regular clean-up tasks as needed. For more details, refer to Configurable tasks.

5. Click **Submit**.

Configurable tasks

Logs exceeding the specified retention period will be automatically deleted.

Login log retention days

User login log retention days.

Task log retention days

Celery task execution record retention days.

Operate log retention days

User operation log retention days.

Password change log retention days

User password change log retention days.

FTP log retention days

FTP file upload and download log retention days.

Session log retention days

Retention days for asset session records, command records, and session recordings (when stored locally). Third-party object storage and command storage are not affected by this setting.

Activity log retention days

Activity log retention days for each resource.

Job execution retention days

Job execution record retention days.

Cloud sync task history retention days

Retention days for execution history of asset cloud synchronization tasks.

Change secret and push record retention days

Retention days for execution records of asset account secret changes and account pushes.

Last updated on November 6, 2025

Import license

This topic describes how to import the license for the enterprise edition of JumpServer.

1. In the right area of the top navigation bar, click ⚙.

2. Navigate to the **System settings** > **License**.

3. In the "Quick update" section on the right side of the page, locate the "Import license" option and click the "Import" button.

4. In the "Import license" dialog box, click the "Choose file" button to select the license file.

5. Click **Confirm**.

Last updated on August 14, 2025

Configuration

This topic describes the configuration options in the config.txt file.

The default location of the file is: `/opt/jumpserver/config/config.txt`

> **Note**
>
> After changing any configuration, run `jmsctl restart` to apply the changes.

SECRET_KEY

Default: (A randomly generated 48-character)

Used to encrypt sensitive information, such as asset account passwords.

Keep the SECRET_KEY same as the old environment during migration. Do not share it with anyone.

BOOTSTRAP_TOKEN

Default: (A randomly generated 24-character)

Used for registration of components such as KoKo, Lion, Magnus, etc.

Keep the BOOTSTRAP_TOKEN same as the old environment during migration. Do not share it with anyone.

DEBUG

Default: `false`

Debug mode shows detailed error pages with full tracebacks and environment info when exceptions occur.

Never enable DEBUG in the production environment for a long time.

DEBUG_DEV

Default: `false`

Debug Dev mode shows more detailed information in log files.

Never enable DEBUG_DEV in the production environment for a long time.

DEBUG_ANSIBLE

Default: `false`

Debug Ansible mode shows more detailed information during task execution.

Never enable DEBUG_ANSIBLE in the production environment for a long time.

LOG_LEVEL

Default: `ERROR`

Control the display of log information at different levels.

- `DEBUG`: Low level system information for debugging purposes.
- `INFO`: General system information.
- `WARNING`: Information describing a minor problem that has occurred.
- `ERROR`: Information describing a major problem that has occurred.
- `CRITICAL`: Information describing a critical problem that has occurred.

DB_ENGINE

Default: `postgresql`

Specifies the backend database engine for JumpServer.

- `postgresql`: Use PostgreSQL as the database.
- `mysql`: Use MySQL or MariaDB as the database.
- `vastbase`: Use Vastbase as the database.

DB_HOST

Default: `postgresql`

The hostname or IP address of the database server. Defaults to the built-in "jms_postgresql" container.

DB_PORT

Default: `5432`

The port number of the database server.

DB_NAME

Default: `jumpserver`

The name of the database to use.

DB_USER

Default: `postgres`

The username used to connect to the database.

DB_PASSWORD

Default: (A randomly generated 26-character)

The password used to connect to the database.

DB_USE_SSL

Default: `false`

Use SSL for the database connection. Supported only with the `mysql` database engine.

The SSL certificate should be placed at `/data/jumpserver/core/data/certs/db_ca.pem`.

REDIS_HOST

Default: `redis`

The hostname or IP address of the redis server. Defaults to the built-in "jms_redis" container.

REDIS_PORT

Default: `6379`

The port number of the redis server.

REDIS_PASSWORD

Default: (A randomly generated 26-character)

The password used to connect to the redis server.

REDIS_USE_SSL

Default: `false`

Use SSL for the Redis connection. If enabled, you need to prepare the following files in advance and place them in the following directory:

- Redis SSL private key file:
  - `/data/jumpserver/core/data/certs/redis_client.key`
- Redis SSL certificate file:
  - `/data/jumpserver/core/data/certs/redis_client.crt`
- Redis SSL CA certificate file (prefer .crt format, .pem as an alternative):
  - `/data/jumpserver/core/data/certs/redis_ca.crt`
  - `/data/jumpserver/core/data/certs/redis_ca.pem`

REDIS_MAX_CONNECTIONS

Default: `100`

The maximum number of connections to the redis server.

REDIS_SENTINEL_HOSTS

Default: (empty)

The Sentinel nodes for redis sentinel mode.

The format is: `ServiceName/host1:port1,host2:port2,host3:port3`

REDIS_SENTINEL_PASSWORD

Default: (empty)

The password used to connect to the redis sentinel nodes.

REDIS_SENTINEL_SOCKET_TIMEOUT

Default: (None)

Specifies the read timeout for redis sentinel connections, in seconds. The default is `none`, which means no timeout.

REDIS_DB_CELERY

Default: `3`

Redis database index used to store celery tasks.

REDIS_DB_CACHE

Default: `4`

Redis database index used for caching.

REDIS_DB_SESSION

Default: `5`

Redis database index used to store user sessions.

REDIS_DB_WS

Default: `6`

Redis database index used for websocket connections.

X_FRAME_OPTIONS

Default: `SAMEORIGIN`

Used to prevent the page from being embedded in third-party sites and to protect users from clickjacking attacks.

- `SAMEORIGIN`: Allows the page to be displayed in a frame on the same origin.
- `DENY`: Prevents the page from being displayed in a frame, regardless of the site attempting to do so.

TOKEN_EXPIRATION

Default: `3600` (in seconds)

The validity period of the bearer token for creating a user through the API, in seconds.

USER_DEFAULT_EXPIRED_DAYS

Default: `25550` (in days)

Default expiration period (in days) for a user. When creating a user, the "Date expired" is automatically calculated based on this setting.

ASSET_PERMISSION_DEFAULT_EXPIRED_DAYS

Default: `25550` (in days)

Default expiration period (in days) for an authorization. When an authorization is created, the "Date expired" is automatically calculated based on this value.

SESSION_COOKIE_DOMAIN

Default: `None`

The domain to use for session cookies. Set this to a string such as "example.com" for cross-domain cookies, or use None for a standard domain cookie.

SESSION_COOKIE_AGE

Default: `86400` (in seconds)

The age of session cookies, in seconds. The default is 24 hours (86400 seconds).

CONNECTION_TOKEN_ONETIME_EXPIRATION

Default: `300` (in seconds)

The validity period of a one-time connection token, in seconds. The default is 5 minutes (300 seconds).

CONNECTION_TOKEN_REUSABLE

default: `false`

Whether to enable reusable connection tokens. The default is false, meaning that each token can only be used once. If set to true, the token can be used multiple times within the validity period.

CONNECTION_TOKEN_REUSABLE_EXPIRATION

Default: `2592000` (in seconds)

The validity period of a reusable connection token, in seconds. The default is 30 days (2592000 seconds).

FACE_RECOGNITION_ENABLED

`enterprise`

Default: `false`

Whether to enable face recognition for user authentication. The facial recognition feature supports the following scenarios:

- MFA authentication during user login.
- Secondary authentication when logging in to an asset.
- Online facial recognition detection after logging in to an asset.

SECURITY_VIEW_AUTH_NEED_MFA

`recommended`

Default: `true`

By default, MFA verification is mandatory when administrators view an asset account's secret.

For more information about configuring the MFA verification validity period, see MFA verify TTL.

VAULT_ENABLED

`enterprise`

Default: `false`

Whether to enable account storage using other vaults (external storage).

VAULT_BACKEND

`enterprise`

Default: `local`

The backend type of the vault. Supported types include:

- `local`: Use JumpServer's built-in database for account storage.
- `hcp`: Use HashiCorp Vault HCP for account storage.
- `azure`: Use Microsoft Azure Key Vault for account storage.
- `aws`: Use Amazon Web Services Secrets Manager for account storage.

VAULT_HCP_HOST

`enterprise`

Default: (empty)

The HCP Vault host address.

VAULT_HCP_TOKEN

`enterprise`

Default: (empty)

The HCP Vault access token.

VAULT_HCP_MOUNT_POINT

`enterprise`

Default: `jumpserver`

The mount point of the secret engine in HCP Vault.

VAULT_AZURE_HOST

`enterprise`

Default: (empty)

The Azure Key Vault host address.

VAULT_AZURE_CLIENT_ID

`enterprise`

Default: (empty)

The Azure Key Vault client ID.

VAULT_AZURE_CLIENT_SECRET

`enterprise`

Default: (empty)

The Azure Key Vault client secret.

VAULT_AZURE_TENANT_ID

`enterprise`

Default: (empty)

The Azure Key Vault tenant ID.

VAULT_AWS_REGION_NAME

`enterprise`

Default: (empty)

The AWS region name where the Secrets Manager is located.

VAULT_AWS_ACCESS_KEY_ID

`enterprise`

Default: (empty)

The AWS access key ID for accessing the Secrets Manager.

VAULT_AWS_ACCESS_SECRET_KEY

`enterprise`

Default: (empty)

The AWS secret access key for accessing the Secrets Manager.

Last updated on October 30, 2025

Enable HTTPS

This topic explains how to configure HTTPS for the JumpServer service to ensure encrypted and secure communication.

1. Log in to the JumpServer deployment server using the "root" or another user with superuser privileges.

2. Place your certificate files in the following directory:

   ```
   /opt/jumpserver/config/nginx/cert
   ```

   Ensure the certificate files are named as follows:

   - server.crt
   - server.key

3. Edit the `config.txt` file and modify the following configuration settings.

   ```
   vi /opt/jumpserver/config/config.txt
   ```

   Change "demo.example.com" to your actual domain name.

   ```
   HTTPS_PORT=443
   SERVER_NAME=demo.example.com
   SSL_CERTIFICATE=server.crt
   SSL_CERTIFICATE_KEY=server.key
   ```

4. Change to the "JumpServer offline package" directory and run the command to restart the service.

   ```
   ./jmsctl.sh restart
   ```

5. Completed.

Last updated on July 8, 2025

JumpServer CE vs EE

This topic describes the feature comparison between the JumpServer open-source edition (JumpServer CE) and the enterprise edition (JumpServer EE).

Resource & Access Management

Feature	JumpServer CE	JumpServer EE
User Management	✓	✓
Role Management	×	✓
Group Management	✓	✓
Asset Management	✓	✓
Cloud Asset Synchronization (AWS, GCP, etc.)	×	✓
Zone Management	✓	✓
Tag Management	✓	✓
Authorization Management	✓	✓
RemoteApp Management (Windows)	✓	✓
VirtualApp Management (Linux)	×	✓
Organizational Management	×	✓

User Authentication Methods

Feature	JumpServer CE	JumpServer EE
LDAP	✓	✓
LDAP HA (High-Availability)	×	✓
CAS	✓	✓
Passkey	✓	✓
OIDC (OpenID Connect)	×	✓
SAML2 (Security Assertion Markup Language 2.0)	×	✓
OAuth2 (Open Authorization 2.0)	×	✓
WeCom (WeChat Work)	×	✓
DingTalk	×	✓
FeiShu	×	✓
Lark	×	✓
Slack	×	✓
RADIUS (Remote Authentication Dial-In User Service)	×	✓

Available Asset Types

Feature	JumpServer CE	JumpServer EE
Unix	✓	✓
Linux	✓	✓
Windows	✓	✓
Network Devices	✓	✓
MariaDB	✓	✓
MySQL	✓	✓
MongoDB	✓	✓
PostgreSQL	✓	✓
Redis	✓	✓
ClickHouse	×	✓
Dameng	×	✓
Oracle	×	✓
SQL Server	×	✓
Kubernetes Clusters	✓	✓
Websites	✓	✓
Basic Remote Applications	✓	✓
Advanced Remote Applications	×	✓

Asset Connection Methods

Feature	JumpServer CE	JumpServer EE
Web-Based SSH Terminal	✓	✓
Web-Based Database Access	✓	✓
Web-Based RDP Access	✓	✓
Web-Based VNC Access	✓	✓
Web-Based Kubernetes Access	✓	✓
Web-Based SFTP File Transfer	✓	✓
Web-Based RemoteApp Access	✓	✓
Web-Based VirtualApp Access	✗	✓
Desktop SSH Client Access	✓	✓
Desktop SFTP Client Access	✓	✓
Desktop Database Client Access	✗	✓
Desktop RDP Client Access	✗	✓
Desktop VNC Client Access	✗	✓
Desktop RemoteApp Access	✗	✓
Desktop VirtualApp Access	✗	✓

Access Control Policies (ACLs)

Feature	JumpServer CE	JumpServer EE
User Login Control	✓	✓
Command Filtering	✓	✓
Asset Connection Control	×	✓
Asset Connection Methods Control	×	✓

Audit & Monitoring Capabilities

Feature	JumpServer CE	JumpServer EE
Asset Session Monitoring	✓	✓
Session Command Auditing	✓	✓
File Transfer Tracking	✓	✓
User Online Device Monitoring	✓	✓
User Login Audit Logs	✓	✓
User Password Change Logs	✓	✓
User Operation Logs	✓	✓

Additional Features & Integrations

Feature	JumpServer CE	JumpServer EE
Email Notifications	✓	✓
SMS Notifications	✗	✓
Ticketing System	✗	✓
Customizable UI Themes	✗	✓

Last updated on August 12, 2025

Changelog

Version	Date	Release Note
v4.10.13	2025-11-20	Read More
v4.10.12	2025-10-27	Read More
v4.10.11	2025-10-21	Read More
v4.10.10	2025-10-16	Read More
v4.10.9	2025-09-24	Read More
v4.10.8	2025-09-18	Read More
v4.10.7	2025-09-04	Read More
v4.10.6	2025-08-29	Read More
v4.10.5	2025-08-21	Read More
v4.10.4	2025-07-17	Read More
v4.10.3	2025-06-30	Read More
v4.10.2	2025-06-19	Read More
v4.10.1	2025-05-19	Read More
v4.10.0	2025-05-15	Read More
v4.9.0	2025-04-17	Read More
v4.8.1	2025-03-28	Read More

Version	Date	Release Note
v4.8.0	2025-03-20	Read More
v4.7.0	2025-02-20	Read More
v4.6.0	2025-01-15	Read More
v4.5.0	2024-12-19	Read More
v4.4.0	2024-11-21	Read More
v4.3.0	2024-10-17	Read More
v4.2.0	2024-09-19	Read More
v4.1.0	2024-08-15	Read More
v4.0.2	2024-08-01	Read More
v4.0.1	2024-07-18	Read More
v4.0.0	2024-07-04	Read More

Last updated on March 31, 2025

FAQ

Why doesn't Ctrl+V enter Visual Block mode in Web Terminal (Luna)?

The Web Terminal (Luna) page is built on xterm.js, and since xterm.js interprets `Ctrl + V` as a paste command, this shortcut cannot be used to enter Vim's Visual Block mode.

Vim provides an alternative shortcut, `Ctrl + Q`, which serves the same purpose and is functionally equivalent to `Ctrl + V` for entering Visual Block mode.

Last updated on November 14, 2025

No available connection methods

Last updated on March 15, 2025