

Managing the Omada Controller

CHAPTERS

1. User Account
2. General Setting
3. History Data Retention
4. Backup&Restore
5. Auto Backup
6. Migrate
7. Information About the Software



This guide applies to:

Omada Controller 3.2.1.

This guide mainly introduces how to manage the user account and configure system settings on Omada Controller.

This chapter includes the following contents.

1. User Account
2. General Setting
3. History Data Retention
4. Backup&Restore
5. Auto Backup
6. Migrate
7. Information About the Software

1 User Account

You can use different user role to log in to the Omada Controller. There are three user roles: administrator, operator and observer. The administration authority varies among different roles.

Administrator	The first administrator account is created in the Basic Configuration process and this account can not be deleted. An administrator can change the settings of the EAP network and create and delete user accounts.
Operator	An operator account can be created or deleted by the administrator. The operator can change the settings of the EAP network.
Observer	An observer account can be created or deleted by the administrator. The observer can only view the status and settings of the EAP network but not change the settings.

Follow the steps below to add a user account.

1. Go to **Controller Settings > User Account**.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Migrate | About

Username, Email, Role

UserName	Email	Role	Created Time	Action
admin	administrator@example.com	administrator	2018-08-03 17:57:15	<input type="checkbox"/>

<< < 1 > >> A total of 1 page(s) Page to:

2. Click **+ Add** and the following window will pop up.

Add User

UserName:

Email: (Optional)

Role: ?

Password:

Confirm Password:

Site Privileges:

3. Specify the username, Email and password of the account.

4. Select the role from the drop-down list.

- If you select **operator** or **observer**, you also need to select the **Site Privileges**.

- If you select **administrator**, the **Site Privileges** option will not appear and all sites are available for the administrator user.

5. Click **Apply** to add the user account.

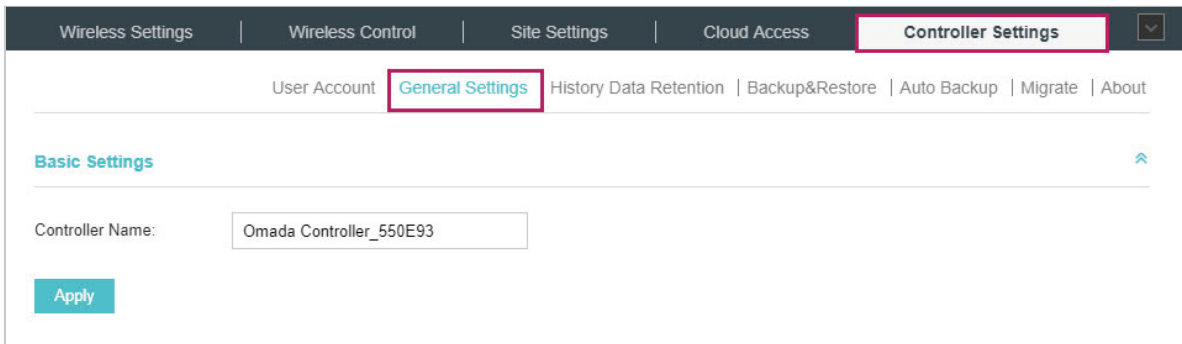
 **Note:**

- You can refer to the **Role** page to view the user role's type, description information, permission scope and created time.
 - The user account cannot be used to log in to the Omada Controller through Omada Cloud Service. To access the controller via Cloud Access, you should be a cloud user. To add a cloud user, refer to [manage the cloud users](#).
-

2 General Setting

2.1 Configure Controller Name

Omada Controller is given a default name in the format **Omada Controller_XXXXXX**. You can give your controller a descriptive name in the **Controller Settings > General Setting** page and click **Apply**.



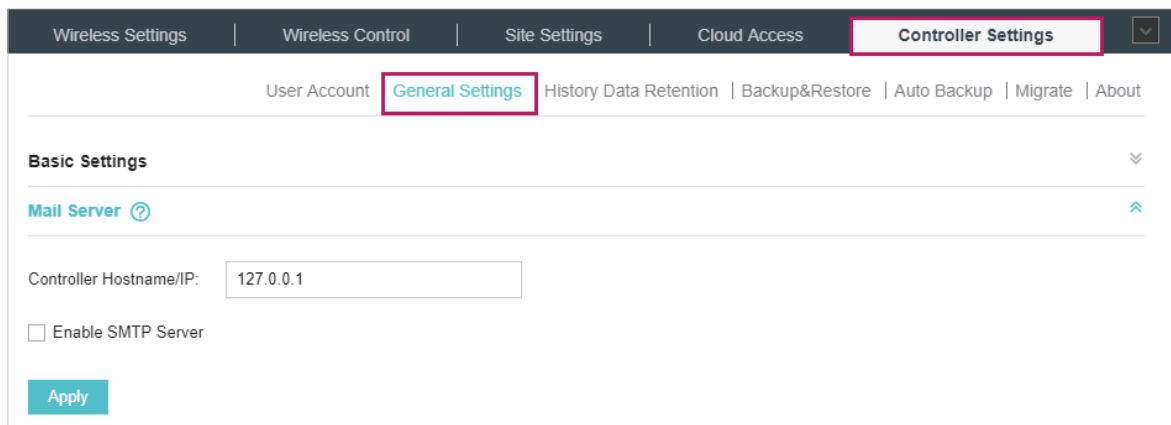
The screenshot shows the Omada Controller web interface. The top navigation bar includes 'Wireless Settings', 'Wireless Control', 'Site Settings', 'Cloud Access', and 'Controller Settings' (highlighted with a red box). Below the navigation bar, the 'General Settings' tab is selected and highlighted with a red box. The 'Controller Name' field contains the text 'Omada Controller_550E93'. An 'Apply' button is visible at the bottom left of the settings area.

2.2 Configure Mail Server

With the Mail Server, you can reset the login password of the user account if necessary. An email with the link of resetting password will be sent from the Omada Controller. It is different from the SMTP Server, which is just for the system log emails sending.

Follow the steps below to configure mail server.

1. Go to **Controller Settings > General Setting** and click **Mail Server**.



The screenshot shows the Omada Controller web interface. The top navigation bar includes 'Wireless Settings', 'Wireless Control', 'Site Settings', 'Cloud Access', and 'Controller Settings' (highlighted with a red box). Below the navigation bar, the 'General Settings' tab is selected and highlighted with a red box. The 'Mail Server' tab is selected and highlighted with a red box. The 'Controller Hostname/IP' field contains the text '127.0.0.1'. There is an unchecked checkbox labeled 'Enable SMTP Server'. An 'Apply' button is visible at the bottom left of the settings area.

2. Enter the hostname or IP address of the Omada Controller. The default IP address of the Omada Controller is **127.0.0.1**. You can keep it or customize the hostname or IP address which can be visited by the Controller host.

When the email with the link of resetting password are sent out, the Controller hostname or IP address will be specified in the Controller URL in every message.

3. Check the box to enable **SMTP Server**, and then the following screen will appear.

The screenshot shows the 'Controller Settings' page with the 'Mail Server' section expanded. The 'Enable SMTP Server' checkbox is checked. The 'Controller Hostname/IP' field contains '127.0.0.1'. The 'Port' field contains '25'. The 'Specify Sender Address' field is empty. The 'Apply' button is visible at the bottom left of the form.

4. Configure the following parameters.

Mail Server	Enter the IP address or domain name of SMTP Server.
Port	The SMTP server uses port 25 as default. You can enable SSL (Security Socket Layer) to enhance secure communications over the Internet. If SSL is enabled, the port number will automatically change to 465.
Enable Auth	Check the box to enable authentication (Optional).
Username/Password	If you enable authentication, enter the username and password required by the mail server.
Specify Sender Address	Specify the sender's mail address. Enter the email address that will appear as the sender for resetting password.

5. Click **Apply** to save the configuration.

 **Note:**

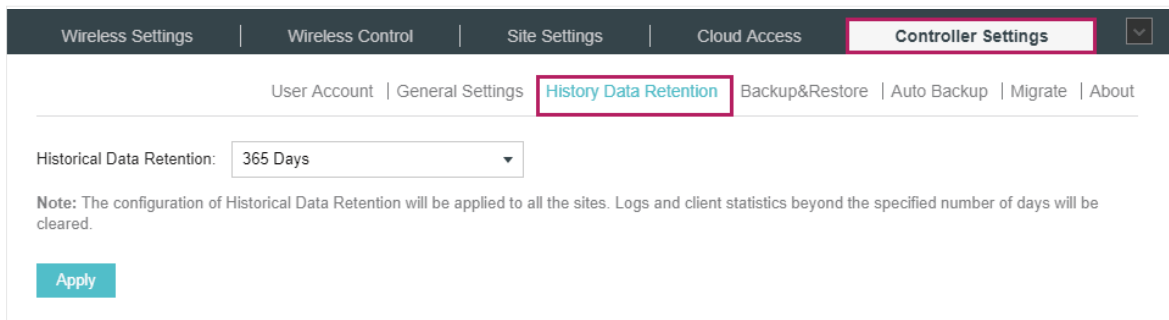
Specify the account email address based on the Mail server to receive the email for resetting password.

3 History Data Retention

History Data Retention allows users to determine the retention of logs and client statistics. The logs and client statistics beyond the specified number of days will be cleared. For example, with **7 days** selected, only the logs and client statistics in recent 7 days will be retained, and the data beyond 7 days will be cleared from the controller.

Follow the steps below to configure Historical Data Retention:

1. Go to **Controller Settings > History Data Retention**.



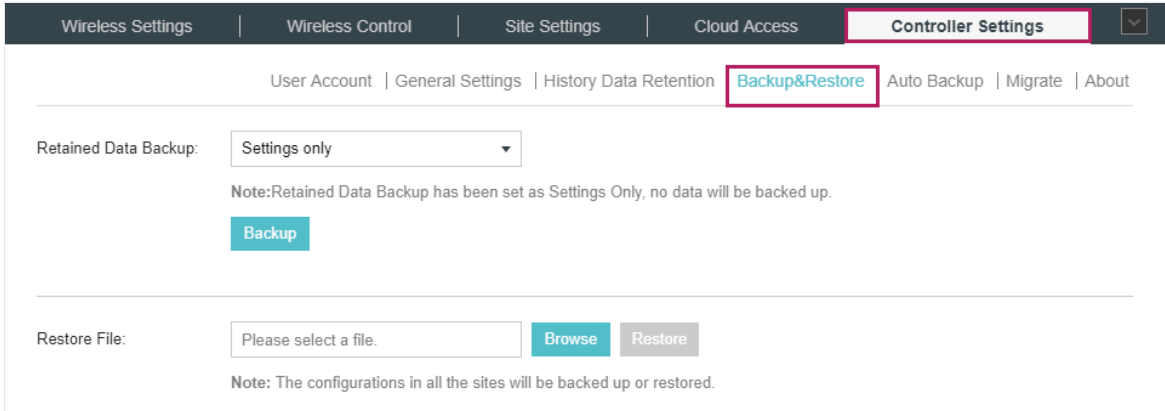
2. Select the length of time in days that data will be retained from the drop-down list. Seven options are provided: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **All time**.
3. Click **Apply**.

4 Backup&Restore

You can save the current configuration and data in the controller as a backup file and if necessary, restore the configuration using the backup file. We recommend that you back up the settings before upgrading the device. This function is available only for local logged-in users.

Follow the steps below to backup and restore the configuration.

1. Go to **Controller Settings > Backup&Restore**.



The screenshot shows the 'Backup&Restore' configuration page within the 'Controller Settings' menu. The page has a dark header with navigation tabs: 'Wireless Settings', 'Wireless Control', 'Site Settings', 'Cloud Access', and 'Controller Settings'. Below the header, there is a breadcrumb trail: 'User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Migrate | About'. The main content area is divided into two sections. The first section, 'Retained Data Backup', features a dropdown menu currently set to 'Settings only'. Below the dropdown is a note: 'Note: Retained Data Backup has been set as Settings Only, no data will be backed up.' and a blue 'Backup' button. The second section, 'Restore File', has a text input field with the placeholder 'Please select a file.', a blue 'Browse' button, and a grey 'Restore' button. A note below this section states: 'Note: The configurations in all the sites will be backed up or restored.'

2. Select the length of time in days that data will be backed up in the **Retained Data Backup** drop-down list. For example, with **7 days** selected, the data only in recent 7 days will be backed up.
3. Click **Backup** to save the backup file.
4. If necessary, click **Browse** to locate and choose the backup file. Then click **Restore** to restore the configuration.

Note:

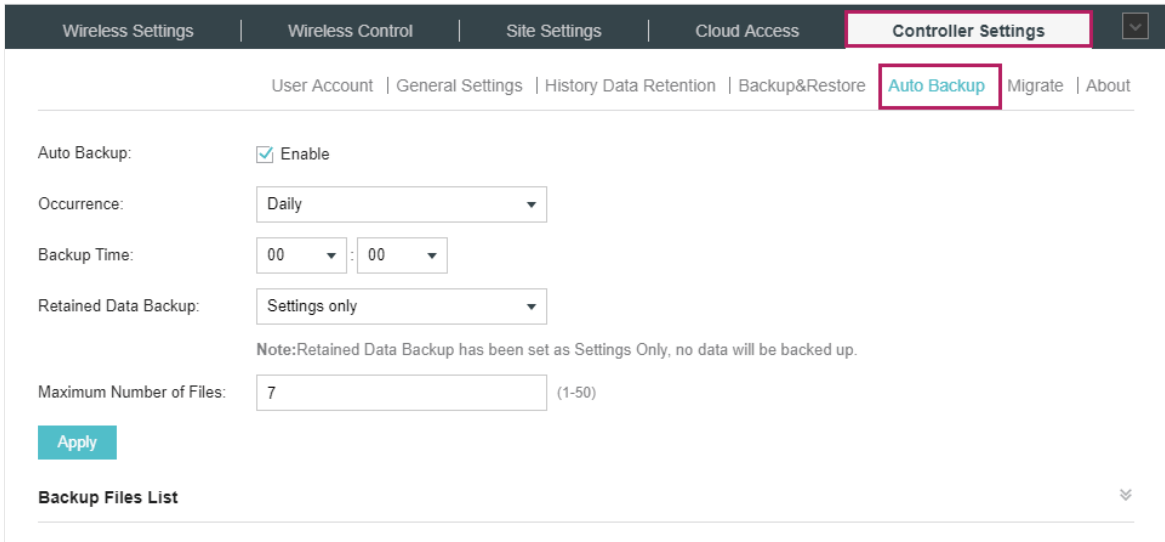
- If you do not want to back up historical data, you can select **Settings only** to get only the controller setting saved in the backup files.
 - If you do not want to back up data manually, you can enable the **Auto Backup** function. Please refer to [Auto Backup](#).
 - To keep the backup data safe , please wait without any operations while restoring the backup file.
-

5 Auto Backup

With Auto Backup enabled, the controller will be scheduled to back up the configuration and data automatically at the specified time.

Follow the steps below to configure Auto Backup function.

1. Go to **Controller Settings > Auto Backup**.



The screenshot shows the 'Controller Settings' page with the 'Auto Backup' sub-tab selected. The configuration options are as follows:

- Auto Backup:** Enable
- Occurrence:** Daily (selected from a dropdown menu)
- Backup Time:** 00 : 00 (selected from two dropdown menus)
- Retained Data Backup:** Settings only (selected from a dropdown menu)
- Note:** Retained Data Backup has been set as Settings Only, no data will be backed up.
- Maximum Number of Files:** 7 (1-50)




An 'Apply' button is located below the settings. At the bottom, there is a section for 'Backup Files List' with a collapse icon.

2. Check the box to enable Auto Backup function.
3. Select how often to perform Auto Backup in the **Occurrence**. You can choose **Daily, Weekly, Monthly** or **Yearly** from drop-down list. Then set an appropriate time to back up files in the **Backup Time**.
When you choose the Occurrence as Monthly, please carefully choose the backup date in Backup Time.
For example, if you choose to automatically backup the data on the 31th day of every month.
When it comes to June, which is only 30 days long, the auto backup will not take effect
4. Select the length of time in days that data will be backed up in the **Retained Data Backup**. For example, with **7 days** selected, the data only in recent 7 days will be backed up.
5. Specify the maximum number of backup files to save in the **Maximum Number of Files**. The default is 7.

You can view the name, backup time and size of the backup files in the **Backup Files List**.

The screenshot shows the 'Controller Settings' page with the 'Auto Backup' section. The 'Auto Backup' checkbox is checked and labeled 'Enable'. The 'Occurrence' is set to 'Weekly'. The days of the week are: Mon (unchecked), Tue (checked), Wed (unchecked), Thu (unchecked), Fri (unchecked), Sat (unchecked), Sun (unchecked). The 'Backup Time' is set to '16:30'. The 'Retained Data Backup' is set to '7 Days'. A note states: 'Note: Retained Data Backup has been set as 7 days, data only in recent 7 days will be backed up.' The 'Maximum Number of Files' is set to '7' (range 1-50). An 'Apply' button is present.

Below the settings is the 'Backup Files List' section, which contains a table with the following data:

File Name	Backup Time	Size	Action
autobackup_7days_20180821_1630.cfg	08/21/2018 16:30	3 KB	  

At the bottom of the table, there are navigation controls: '<<' '<' '1' '>' '>>' and a page indicator 'A total of 1 page(s) Page to: [input] GO'.

You can execute the corresponding operation to the backup files by clicking an icon in the Action column.



Restore the data and configurations in the backup file.



Download the backup file.



Delete the backup file.

 **Note:**

- To back up data manually and restore the data to the controller, configure **Backup&Restore** function. Please refer to [Backup&Restore](#).
- If you do not want to back up historical data, you can select **Settings only** to get only the controller setting saved in the backup files.
- The auto backup files will be stored in data/ autobackup folder of the controller installation location.
- The configuration of the cloud users will not be backed up. Thus the configuration of the cloud users cannot be restored. To add cloud users, please refer to [Manage the Cloud Users](#).
- To keep the backup data safe , please wait without any operations while restoring the backup file.

6 Migrate

Migrate function allows users to migrate the configurations and data to any other site or controller.

For Migrating all the configurations and data from the current controller to any other controller, refer to [Controller Migrate](#).

For Migrating the configurations and data from the existing site to any other controller, refer to [Site Migrate](#).

6.1 Controller Migrate

With Controller Migrate function, you can migrate your configurations and data from the current controller to any other controller that has the same or higher version.

The process of migrating configurations and data from the current controller to another controller can be summarized in three steps: Export Controller, Migrate Controller and Migrate Devices.

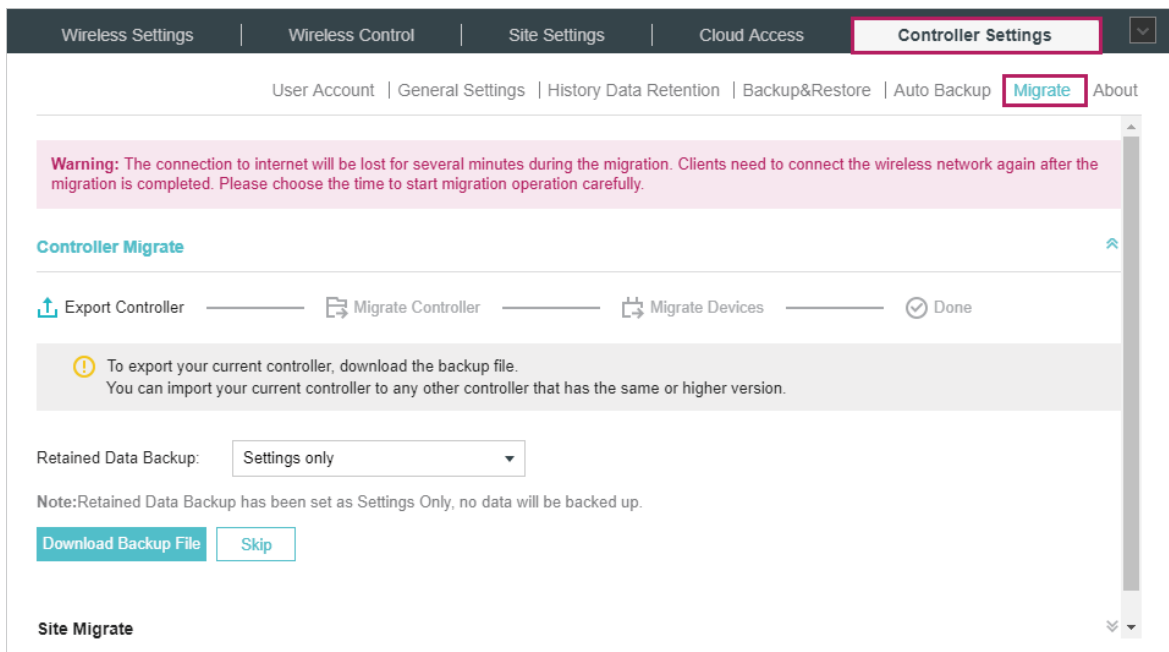
Follow the steps below to migrate your controller.

 **Note:**

- The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.
- Exporting Controller and Migrating Controller are available only for local logged-in users.

■ **Export Controller**

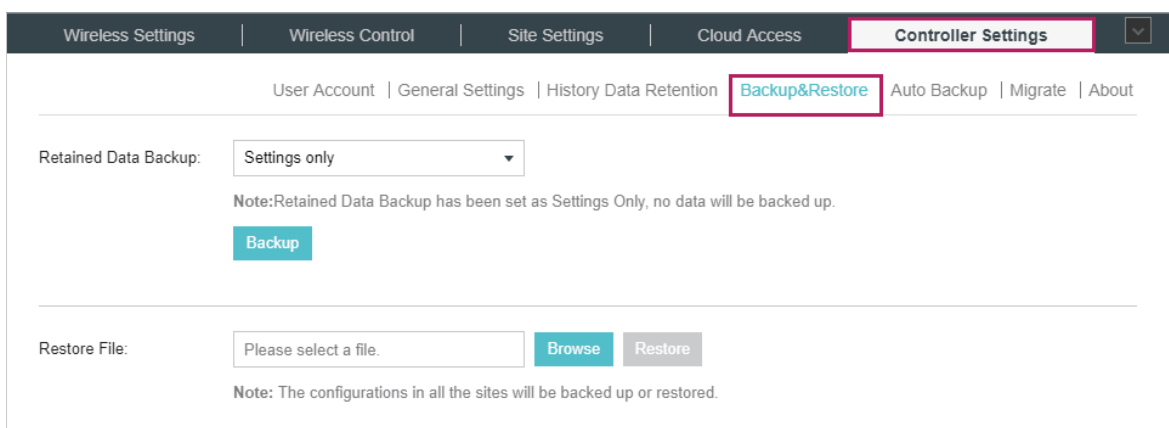
1. Go to **Controller Settings > Migrate > Controller Migrate**.



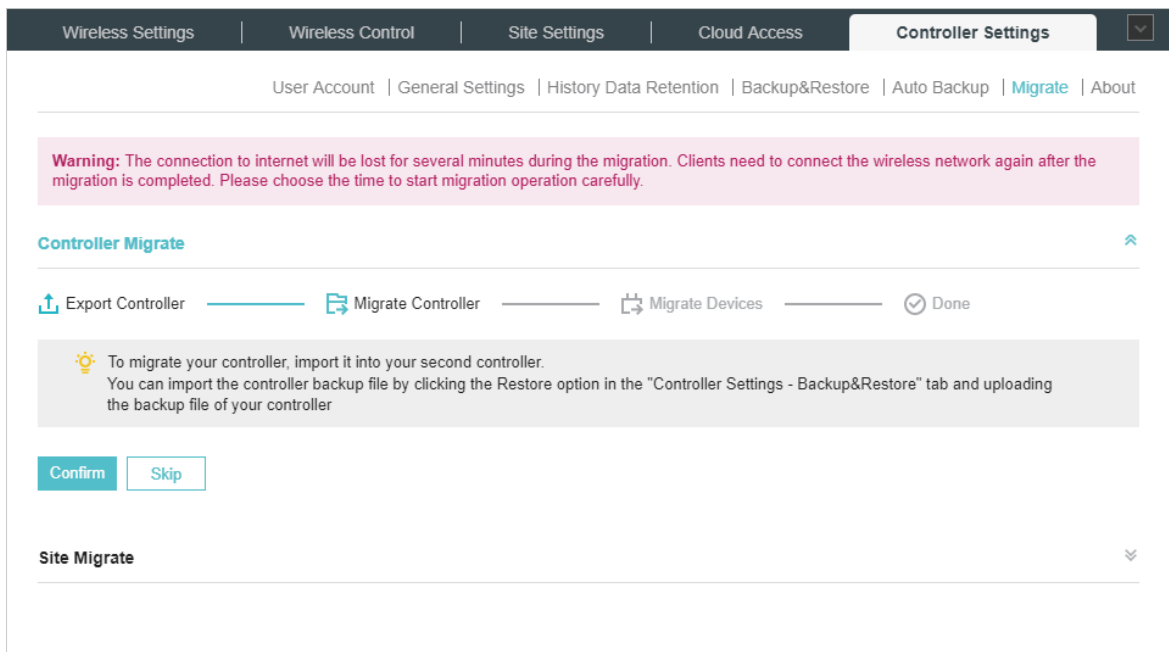
2. Select the length of time in days that data to be imported into the second controller in the **Retained Data Backup** drop-down list. For example, with **7 days** selected, the data only in recent 7 days will be imported into the second controller.
3. Click **Download Backup File** to download the file of the current controller. If you have backed up the file, click **Skip**.

■ Migrate Controller

1. Start and log in to the second controller, go to **Controller Settings > Backup&Restore > Restore File**.

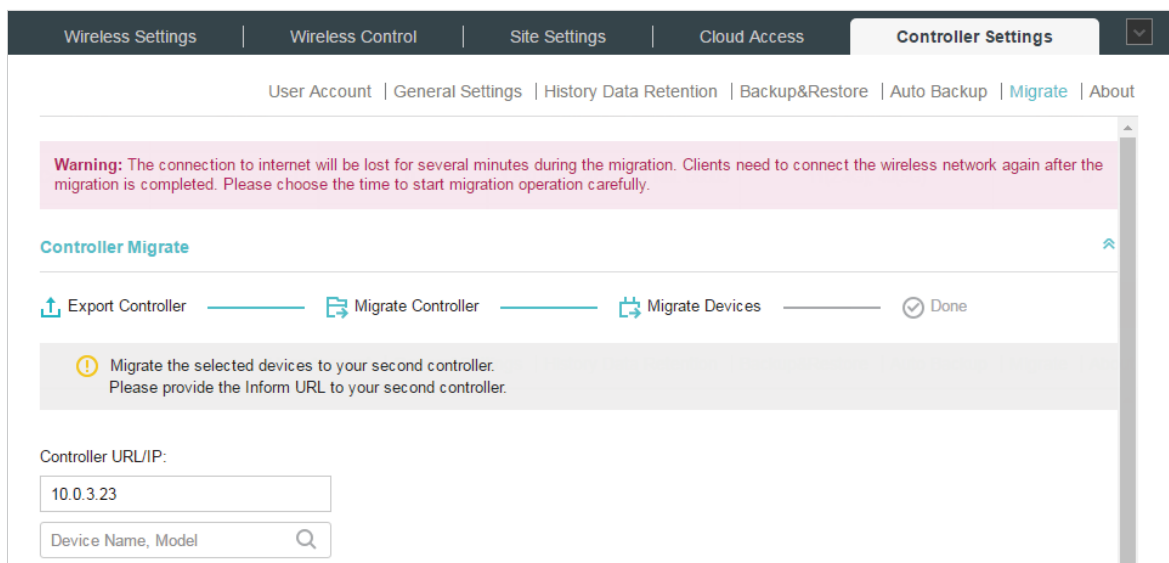


2. Click **Browse** to locate and choose the file of your controller to be imported. Then click **Restore** to upload the file.
3. After the file has been restored to the second controller, go back to the export controller and click **Confirm**.



■ Migrate Devices

1. Enter the IP address or URL of your second controller into **Controller URL/IP** input field. In this case, the IP address of the second controller is 10.0.3.23.



Note:

Make sure that you enter the correct IP address of the second controller to establish the communication between EAPs and your second controller. Otherwise the EAPs cannot be adopted by the second controller.

2. Select the devices that are to be migrated by clicking the boxes next to each devices. By default, all the devices are selected.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | [Migrate](#) | About

Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate

Export Controller ———— Migrate Controller ———— Migrate Devices ———— Done

⚠️ Migrate the selected devices to your second controller. Please provide the Inform URL to your second controller.

Controller URL/IP:

Device Name, Model

<input checked="" type="checkbox"/>	↕ Device Name	↕ Site	↕ Status	↕ Model	↕ Hardware Version
<input checked="" type="checkbox"/>	EA-23-51-06-22-52	Default	Connected	EAP225-Outdoor(EU)	1.0
<input checked="" type="checkbox"/>	EA-33-51-A8-22-A0	Default	Connected	EAP225-Outdoor(EU)	1.0

Selected 2 of 2 items. << < 1 > >> A total of 1 page(s) Page to: **GO**

Migrate Devices

3. Click **Migrate Devices** to migrate the selected devices to the second controller.
4. Verify that all the migrated devices are visible and connected on the second controller. Note that this may take several minutes. When all the migrated devices are in **Connected** status on the **Access Points** page on the second controller, click **Forget Devices** to finish the migration process.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | [Migrate](#) | About

⚠️ To finish the migration process, forget the successfully migrated devices. Please visit the device page in your second controller and check if all of the migrated devices are visible and connected. This process may take several minutes.

Device Name, Model

<input checked="" type="checkbox"/>	↕ Device Name	↕ Site	↕ Status	↕ Model	↕ Hardware Version
<input checked="" type="checkbox"/>	EA-23-51-06-22-52	Default	Connected	EAP225-Outdoor(EU)	1.0
<input checked="" type="checkbox"/>	EA-33-51-A8-22-A0	Default	Connected	EAP225-Outdoor(EU)	1.0

Selected 2 of 2 items. << < 1 > >> A total of 1 page(s) Page to: **GO**

Forget Devices

When the migration process is completed, all the configuration and data are migrated to the second controller. You can uninstall the previous controller if necessary.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | [Migrate](#) | About

Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate

Export Controller — Migrate Controller — Migrate Devices — Done

⚠ To finish the migration process, forget the successfully migrated devices.
Please visit the device page in your second controller and check if all of the migrated devices are visible and connected. This process may take several minutes.

Device Name, Model 🔍

<input type="checkbox"/>	↕ Device Name	↕ Site	↕ Status	↕ Model	↕ Hardware Version
No entry in the table.					

Selected 0 of 0 items. << < > >> A total of NaN page(s) Page to: **GO**

6.2 Site Migrate

With Site Migrate function, you can migrate your configurations and data of a site to any other controller that has the same version.

The process of migrating configurations and data from a site to another controller can be summarized in three steps: Export Site, Migrate Site and Migrate Devices.

Follow the steps below to migrate a site to another controller.

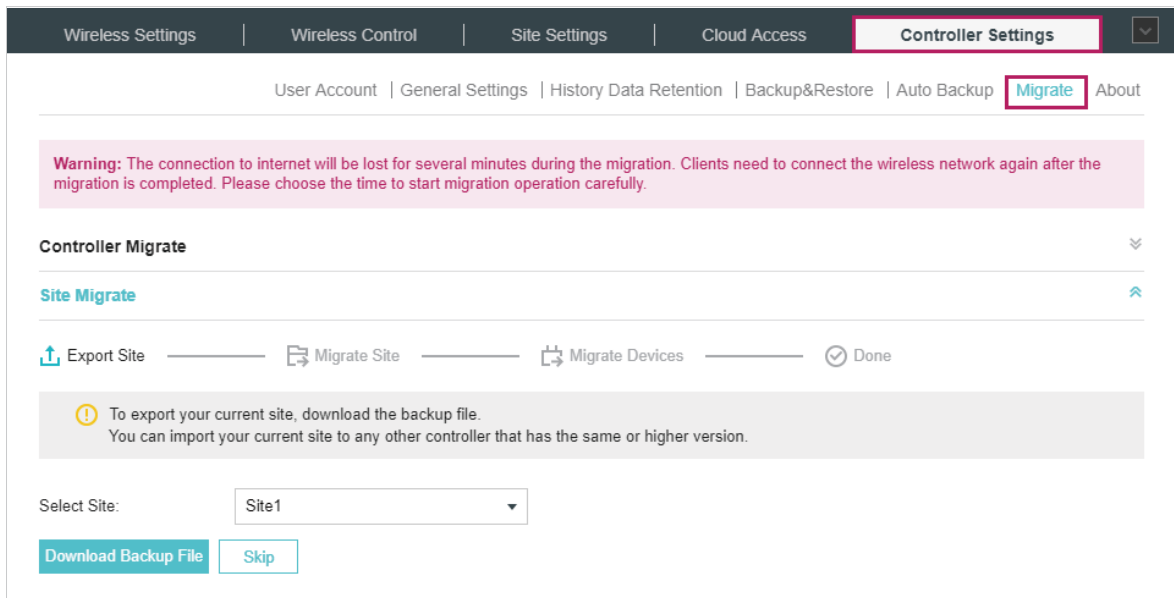


Note:

The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

■ Export Site

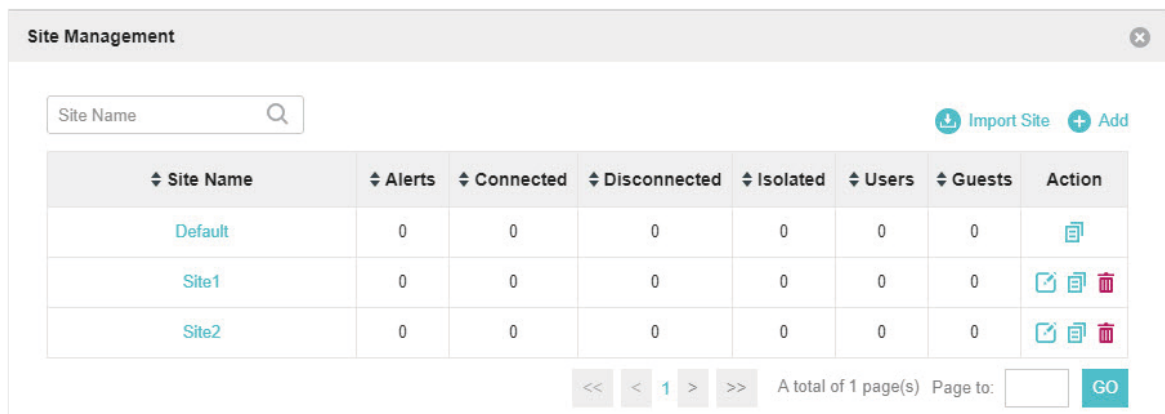
1. Go to **Controller Settings > Migrate > Site Migrate**.



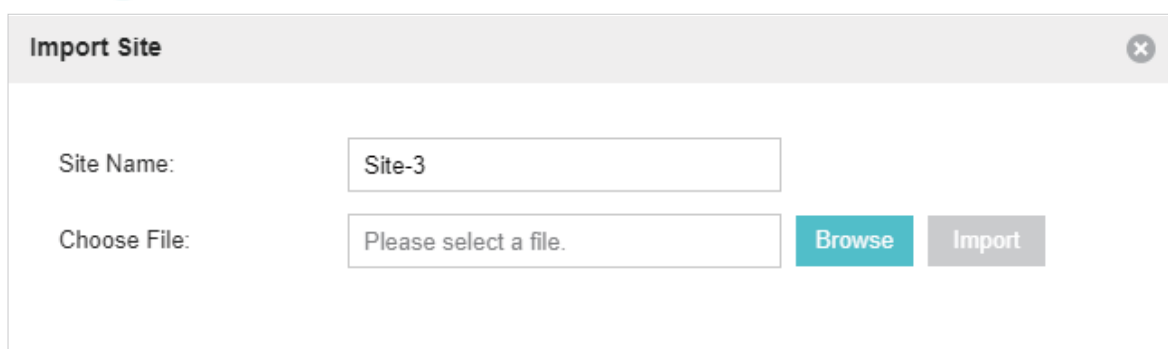
2. Select the site to be imported into the second controller in the **Select Site** drop-down list.
3. Click **Download Backup File** to download the file of the current site. If you have backed up the file, click **Skip**.

■ Migrate Site

1. Start and log in to the second controller, click **Sites: Default** in the top left corner of the page and select **Site Manager**, and then the following window will pop up.



2. Click **Import Site** and enter a unique name for the new site.



3. Click **Browse** to upload the file of the site to be imported and click **Import** to import the site.

Import Site
✕

Site Name:

Choose File: Browse Import

4. After the file has been imported to the second controller, go back to the export controller and click **Confirm**.

Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Migrate | About

Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate ⌵

Site Migrate ⌴

⬆ Export Site
⬆ Migrate Site
⬆ Migrate Devices
⌵ Done

⚠ To migrate your site, import it into your second controller.
You can import the site by clicking the Import Site in the "Site Management" drop down and uploading the backup file of your site.

Confirm
Skip

■ Migrate Devices

1. Enter the IP address or URL of your second controller into **Controller URL/IP** input field. In this case, the IP address of the second controller is 10.0.3.14.

Wireless Settings
Wireless Control
Site Settings
Cloud Access
Controller Settings

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Migrate | About

Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate ⌵

Site Migrate ⌴

⬆ Export Site
⬆ Migrate Site
⬆ Migrate Devices
⌵ Done

⚠ Migrate the selected devices to your second controller.
Please provide the Inform URL to your second controller.

Controller URL/IP:

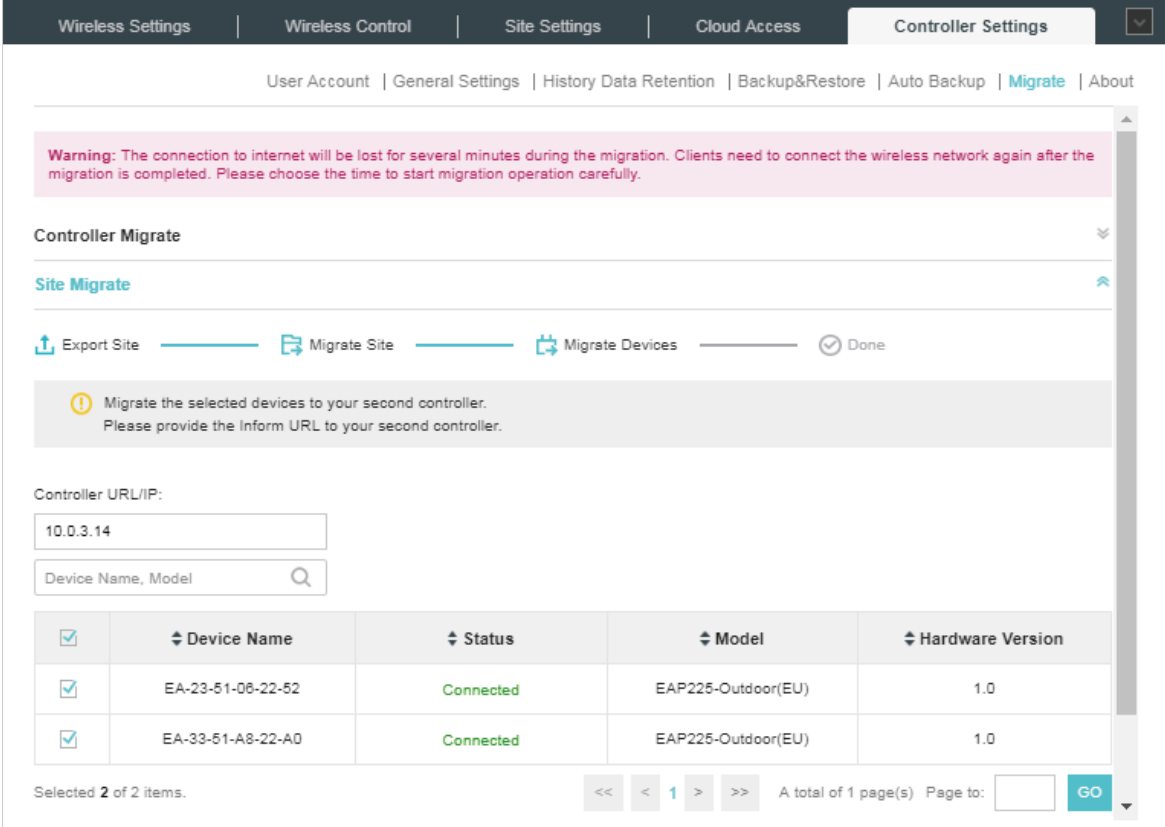
🔍

<input checked="" type="checkbox"/>	↕ Device Name	↕ Status	↕ Model	↕ Hardware Version

 **Note:**

Make sure that you enter the correct IP address of the second controller to establish the communication between EAPs and your second controller. Otherwise the EAPs cannot be adopted by the second controller.

2. Select the devices that are to be migrated by clicking the boxes next to each devices. By default, all the devices are selected.



Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate

Site Migrate

Export Site — Migrate Site — Migrate Devices — Done

Migrate the selected devices to your second controller.
Please provide the Inform URL to your second controller.

Controller URL/IP:
10.0.3.14

Device Name, Model

<input checked="" type="checkbox"/>	Device Name	Status	Model	Hardware Version
<input checked="" type="checkbox"/>	EA-23-51-06-22-52	Connected	EAP225-Outdoor(EU)	1.0
<input checked="" type="checkbox"/>	EA-33-51-A8-22-A0	Connected	EAP225-Outdoor(EU)	1.0

Selected 2 of 2 items. << < 1 > >> A total of 1 page(s) Page to: GO

3. Click **Migrate Devices** to migrate the selected devices to the second controller.
4. Verify that all the migrated devices are visible and connected on the second controller. Note that this may take several minutes. When all the migrated devices are in **Connected** status on the **Access Points** page on the second controller, click **Forget Devices** to finish the migration process.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | [Migrate](#) | About

⚠ To finish the migration process, forget the successfully migrated devices.
Please visit the device page in your second controller and check if all of the migrated devices are visible and connected. This process may take several minutes.

Device Name, Model

<input checked="" type="checkbox"/>	↕ Device Name	↕ Site	↕ Status	↕ Model	↕ Hardware Version
<input checked="" type="checkbox"/>	EA-23-51-06-22-52	Default	Connected	EAP225-Outdoor(EU)	1.0
<input checked="" type="checkbox"/>	EA-33-51-A8-22-A0	Default	Connected	EAP225-Outdoor(EU)	1.0

Selected 2 of 2 items. << < 1 > >> A total of 1 page(s) Page to: **GO**

Forget Devices

When the migration process is completed, all the configuration and data are migrated to the second controller. You can delete the previous site if necessary.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings**

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | [Migrate](#) | About

Warning: The connection to internet will be lost for several minutes during the migration. Clients need to connect the wireless network again after the migration is completed. Please choose the time to start migration operation carefully.

Controller Migrate

Site Migrate

Export Site — Migrate Site — Migrate Devices — Done

⚠ To finish the migration process, forget the successfully migrated devices.
Please visit the device page in your second controller and check if all of the migrated devices are visible and connected. This process may take several minutes.

Device Name, Model

<input type="checkbox"/>	↕ Device Name	↕ Status	↕ Model	↕ Hardware Version
No entry in the table.				

7 Information About the Software

You can view the Omada Controller's version and copyright information on the **Controller Settings > About** page.

Wireless Settings | Wireless Control | Site Settings | Cloud Access | **Controller Settings** ▾

User Account | General Settings | History Data Retention | Backup&Restore | Auto Backup | Migrate | **About**

Version: 3.1.13
Copyright © 2013-2019 TP-Link Technologies Co., Ltd.
All rights reserved.