### Account

#### Overview

The account feature provides the ability to register and manage users in Logpresso Sonar. All users can access the web console and the [REST API](https://docs.logpresso.comnull) within the scope of the data granted by their assigned roles and access rights.

Account Roles

The account roles are as follows:

* **Cluster Administrator**: The default administrator account provided upon installation of Logpresso Sonar. It has full configuration rights, including server cluster settings.
* **Administrator**: Has all configuration, data, and account management rights, excluding those of the Cluster Administrator.
* **User**: Has the right to view only the data that the (Cluster) Administrator has permitted access to.
* **Dashboard Publisher**: Has the right to view only the data necessary for sharing Logpresso Sonar dashboards externally.

2FA

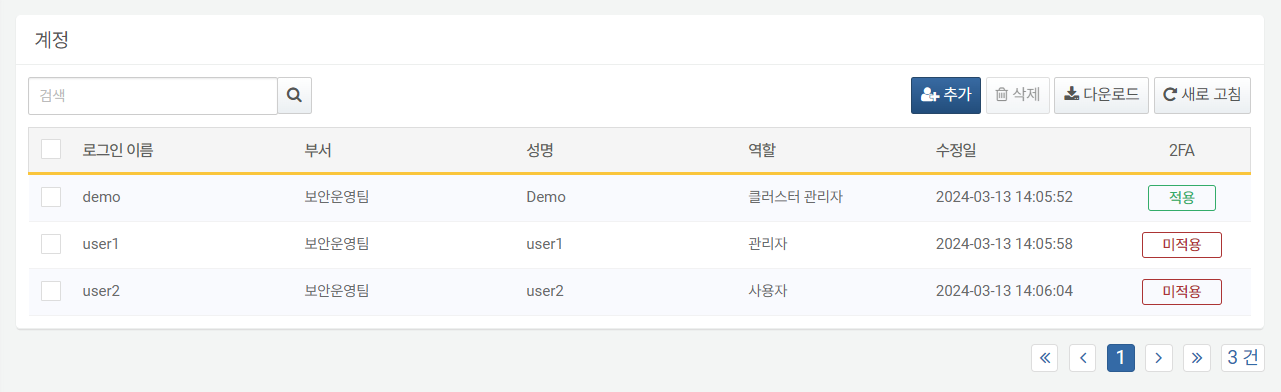
Two-factor authentication (2FA) can be applied when logging into an account to enhance security. Currently, only OTP is supported. Any OTP app that complies with Google Authenticator or [RFC 6238](https://datatracker.ietf.org/doc/html/rfc6238) can be used.

API Key

An API key is required to use the Logpresso REST API. API keys are generated on a per-account basis and have permissions based on the roles assigned to the account.

#### Viewing/Search Account List

Cluster Administrators and Administrators can view the account list on the **Accounts > Accounts** screen. User accounts cannot view the account list.



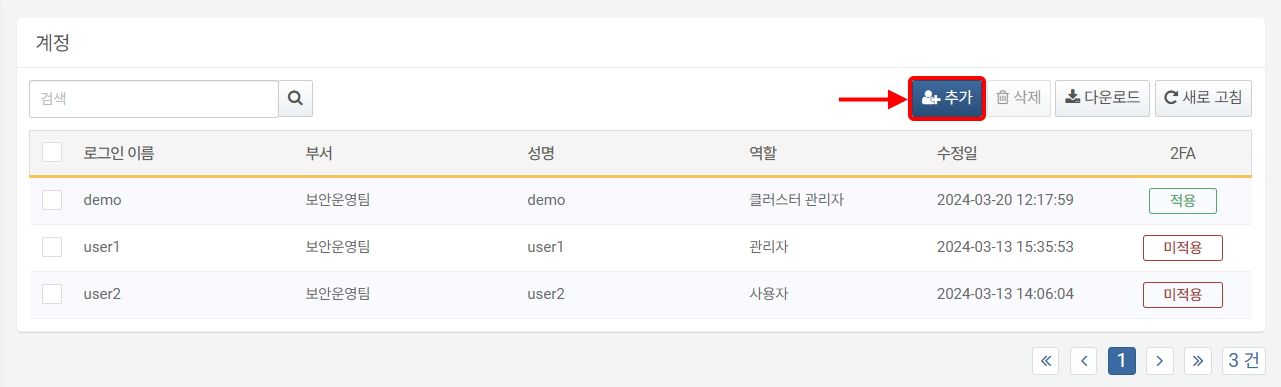
To find a specific account in the account list, use the search tool in the toolbar. The search tool will display accounts that contain the entered words in **Login Name**, **Department**, or **Full Name**. The search tool is case-sensitive.



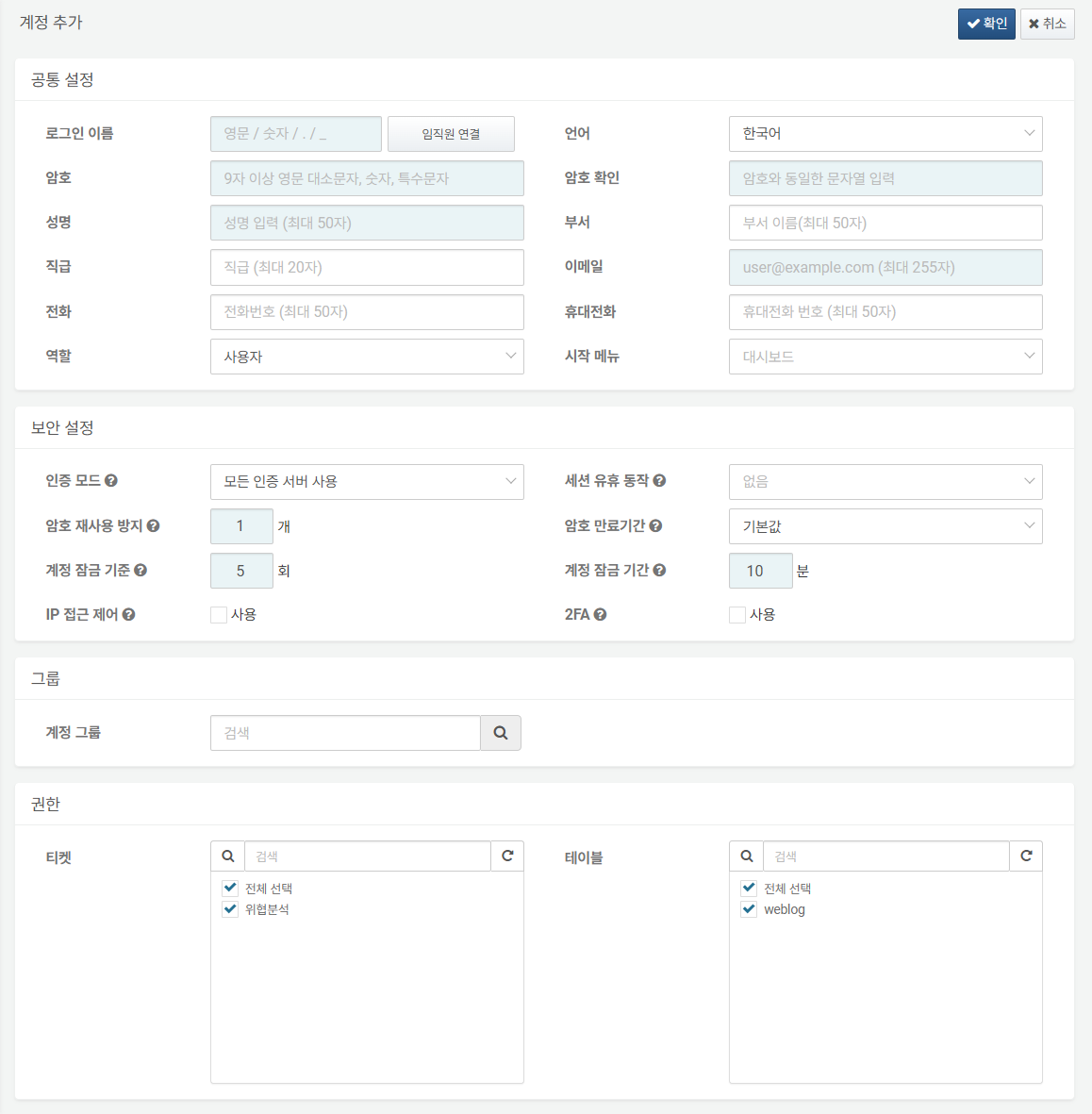
#### Adding an Account

To add a new account:

Click **Add** in the toolbar on the **Accounts > Accounts** screen.



In the **Add Account** screen, enter or select the properties for [Common Settings](https://docs.logpresso.comnull), [Security Settings](https://docs.logpresso.comnull), [Groups](https://docs.logpresso.comnull), and [Permissions](https://docs.logpresso.comnull). Properties highlighted in sky blue are mandatory fields.

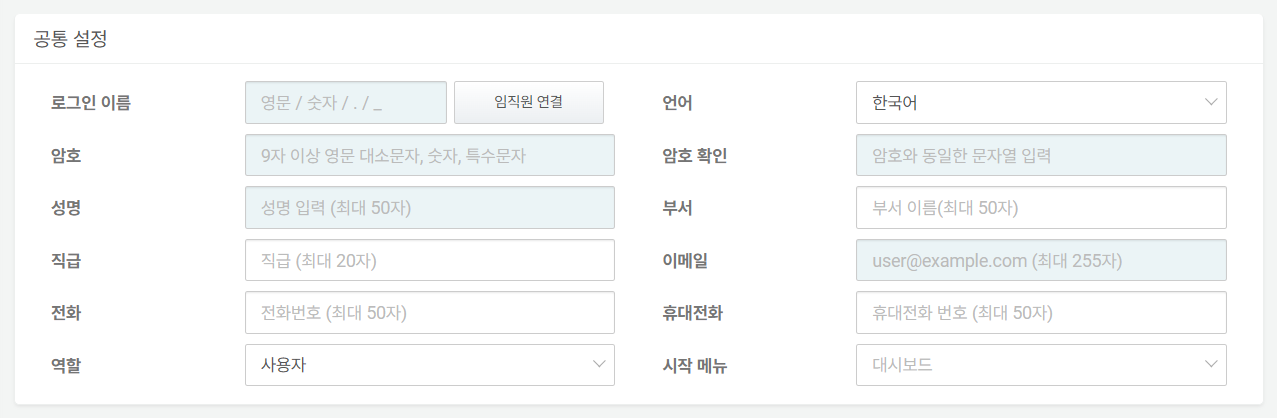


Review the entered or selected properties for correctness and click **Confirm** in the upper right corner.

The following content describes the information required for account settings.

Common Settings

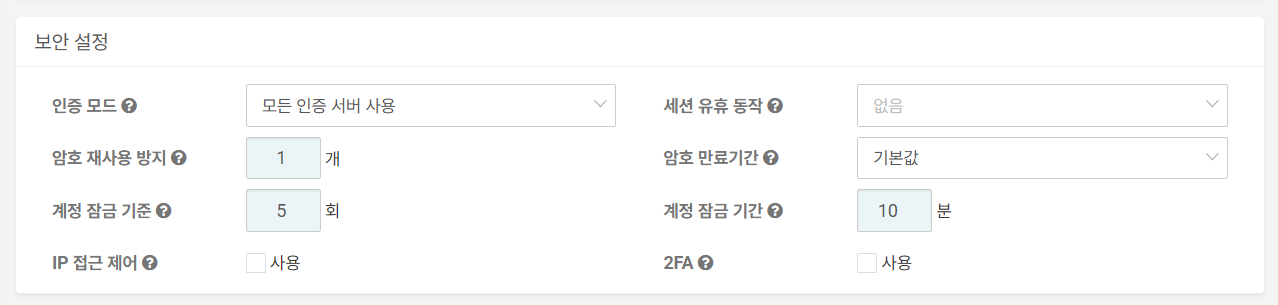
General unique settings for the account.

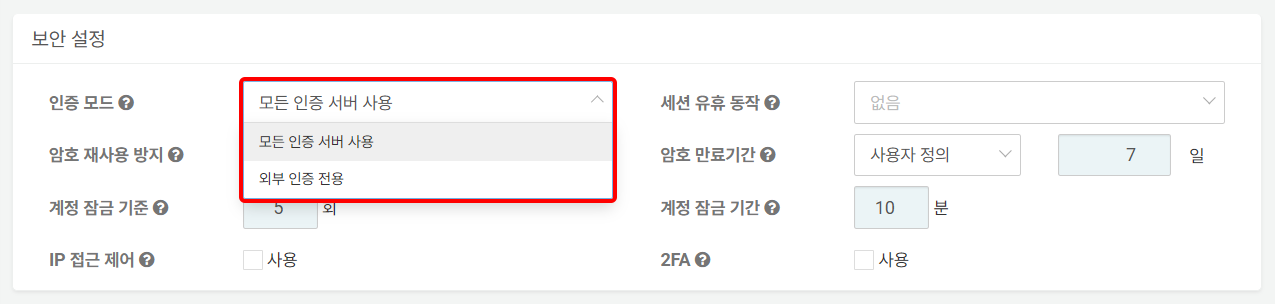
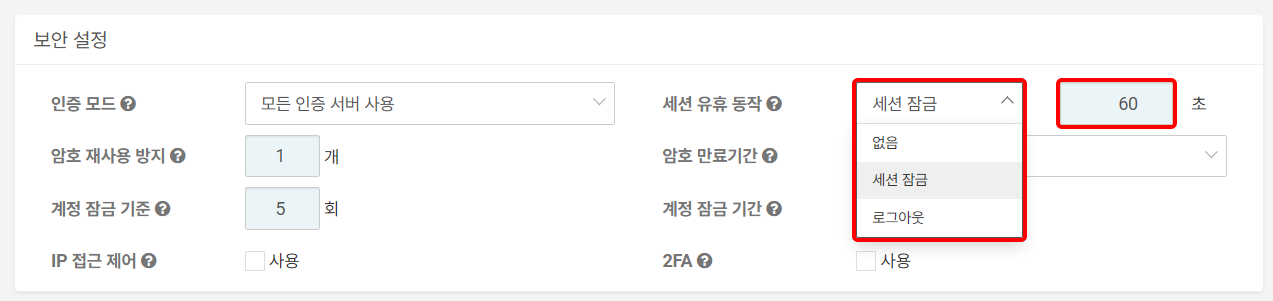
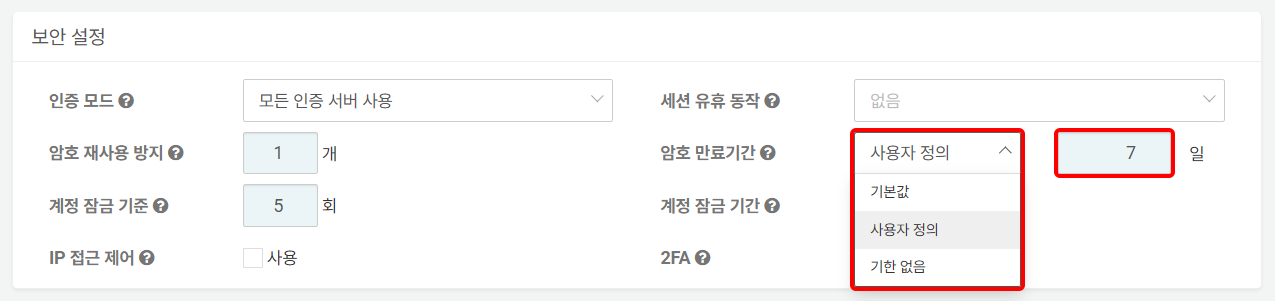


* **Login Name**: The ID used to log into Logpresso Sonar. The login name can only contain English letters (case-sensitive), numbers, periods (.), and underscores (\_).
* After entering the login name, clicking **Connect Employees** will search for the **Employee Number** that matches the **Login Name** from the registered [Employees](https://docs.logpresso.comnull) information and automatically fill in **Full Name**, **Email**, **Language**, **Department**, **Position**, **Phone**, and **Mobile Phone** information.
* **Language**: The language to be applied in the web console after logging into Logpresso Sonar. Choose between **Korean** and **English**.
* **Password, Confirm Password**: The password to be used for authentication when logging in. Enter the same value in both the **Password** and **Confirm Password** fields. The password must be at least 9 characters long and include uppercase and lowercase letters, numbers, and special characters.
* **Full Name**: The actual name of the user.
* **Department**: The department to which the user belongs.
* **Position**: The user's position information.
* **Email**: The email address to receive emails sent by Logpresso Sonar.
* **Phone**: The user's phone number.
* **Mobile Phone**: The user's mobile phone number. If SMS is configured to be sent to the user by Logpresso Sonar, the registered mobile phone number can be used.
* **Role**: Select the account's [role](https://docs.logpresso.comnull) from **Cluster Administrator**, **Administrator**, **User**, or **Dashboard Publisher** (default: User).
* **Start Menu**: The screen to be used as the start page in the session of the logged-in account in the web console (default: Dashboard).

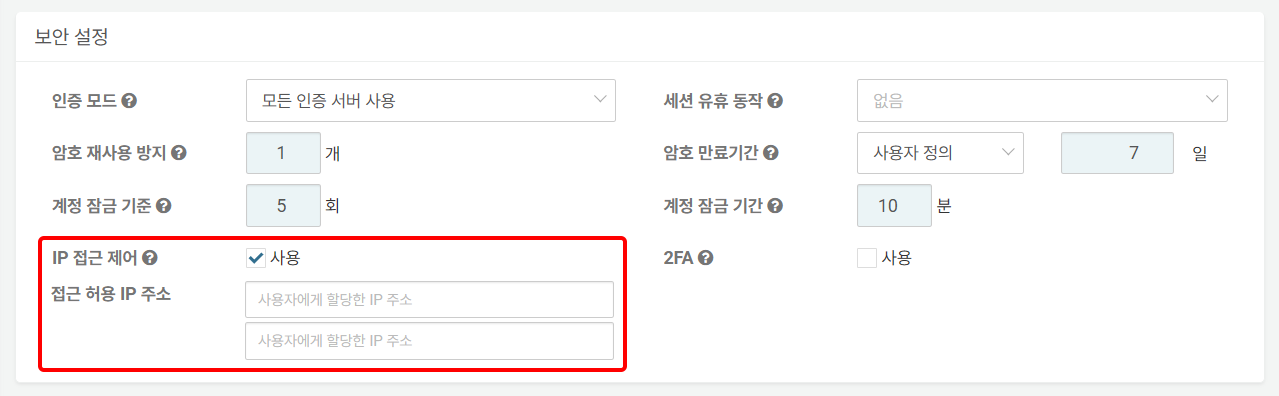
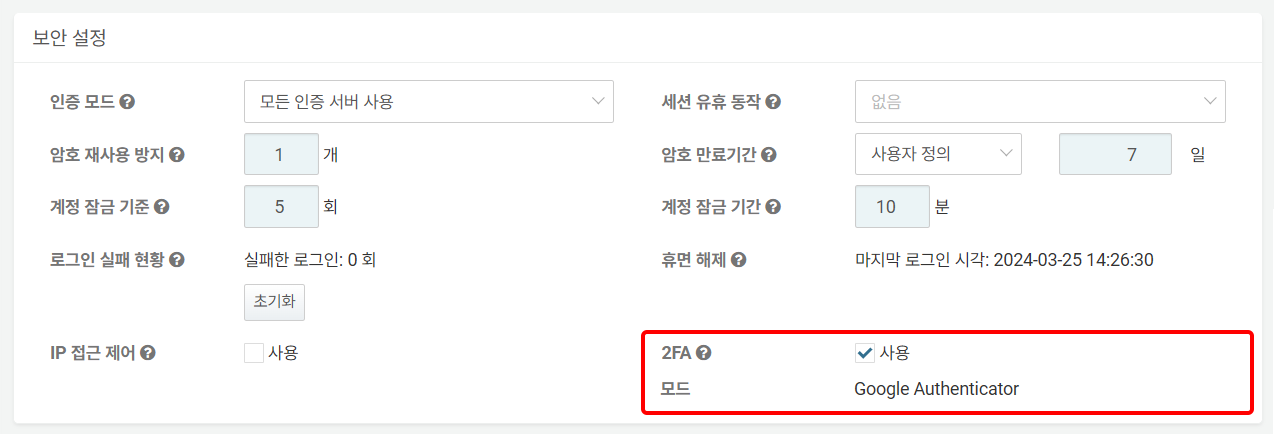
Security Settings

Various security settings for the account.



* **Authentication Mode**: Select the server to be applied for account authentication (default: Use all authentication servers).
* 
* **Use all authentication servers**: Attempts to authenticate the account matching the login name from all authentication servers configured on the server. It first attempts local account authentication registered on the server, followed by external authentication servers. The login names for local accounts and external authentication servers must be the same.
* **External authentication only**: Authenticates the account using the authentication information provided by external authentication servers.
* **Session Idle Action**: The policy to apply to the session when the user does not use the account for a certain period. Choose from **None**, **Lock**, or **Logout** (default: None). If **Lock** or **Logout** is selected, the default idle time applied is 60 seconds. The idle time can be set to a value between 60 and 604,800 seconds (1 week).
* 
* **Prevent Password Reuse**: A policy that prevents users from using previous passwords when changing their login password. The server remembers the hash values of the passwords used for the account for a specified number of times and blocks reuse (default: 1, valid range: 0-23).
* **Password Expiration Period**: The period during which the password can be used after being set. Choose from **Default** (365 days), **Custom**, or **No Expiration**. The server will display a password change popup when logging in and unlocking the session starting 7 days before the password expiration.
* 
* **Default**: 365 days
* **Custom**: 7 days is the default, and it can be set between 7 and 3,650 days.
* **No Expiration**: No expiration period is specified for the password.

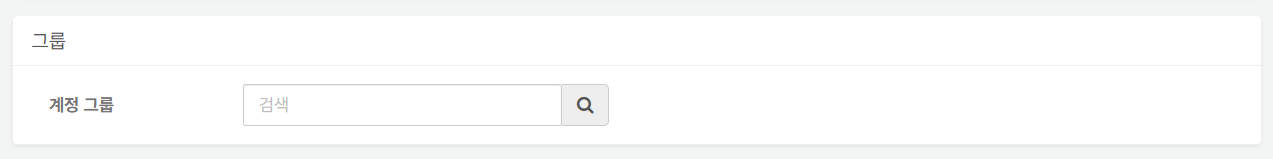
: If a user attempts to log in with an expired password, the password change window will appear as shown below.

* **Account Lock Criteria**: The number of consecutive failed login attempts. If the user fails to log in the specified number of times, the account will be locked, and login will be blocked (default: 5, maximum: 50). Specifying '0' means that account locking will not be applied.
* **Account Lock Duration**: The duration for which the user's account lock will be applied. The default is 10 minutes, and the maximum is 100,000,000 minutes (approximately 39 months).
* **IP Access Control**: Used to restrict the IP addresses from which the account can log in (default: Disabled). Checking **Enable** will display the **Allowed IP Addresses** input field, where a maximum of 2 IP addresses can be specified.
* 
* **2FA**: Whether to apply 2FA (default: Disabled). The currently supported mode for 2FA is OTP. Any OTP app that complies with Google Authenticator or [RFC 6238](https://datatracker.ietf.org/doc/html/rfc6238) can be used.
* 

: For information on how account users can log in using 2FA, refer to [here](https://docs.logpresso.comnull).

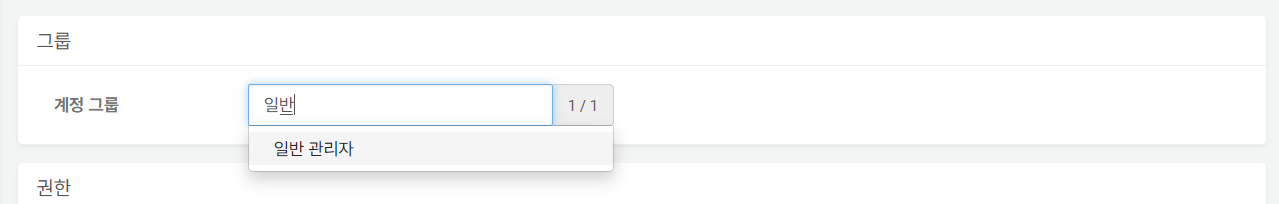
Groups

In **Groups**, you can search for account groups and assign accounts to account groups.

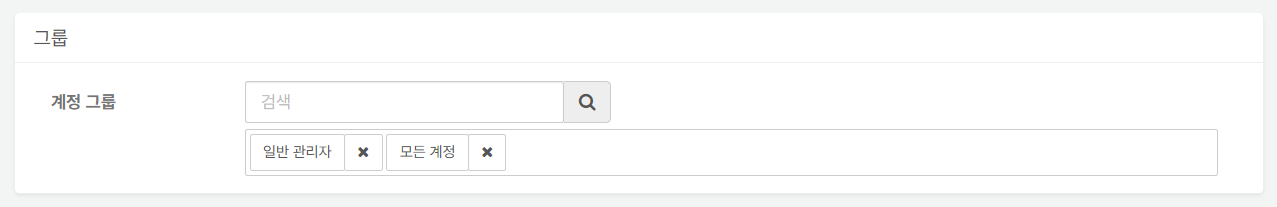


To assign a group to an account:

Enter the name of the account group to which you want to assign the account in the account group field. A list of account groups containing the entered string will appear; click the account group to which you want to assign the account.



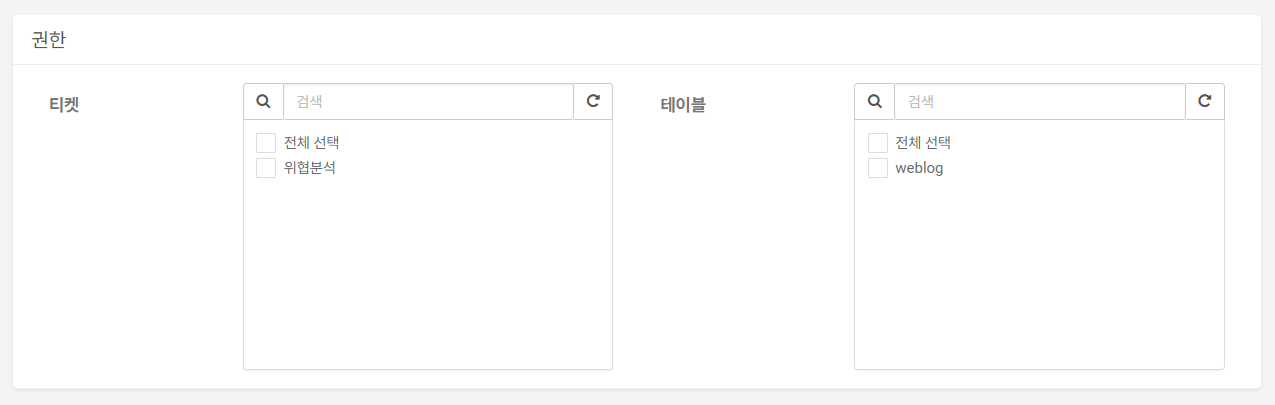
To assign to more than one account group, repeat the above steps.



To remove a user from the assigned account group, click the X next to the account group name.

Permissions

Permissions allow you to select [Ticket Repositories](https://docs.logpresso.comnull) and [Tables](https://docs.logpresso.comnull) to grant access rights to the account. When the role assigned to the account is User or Dashboard Publisher, access is granted only to the specified ticket repositories and tables. Cluster Administrators and Administrators have access to all tickets and tables.

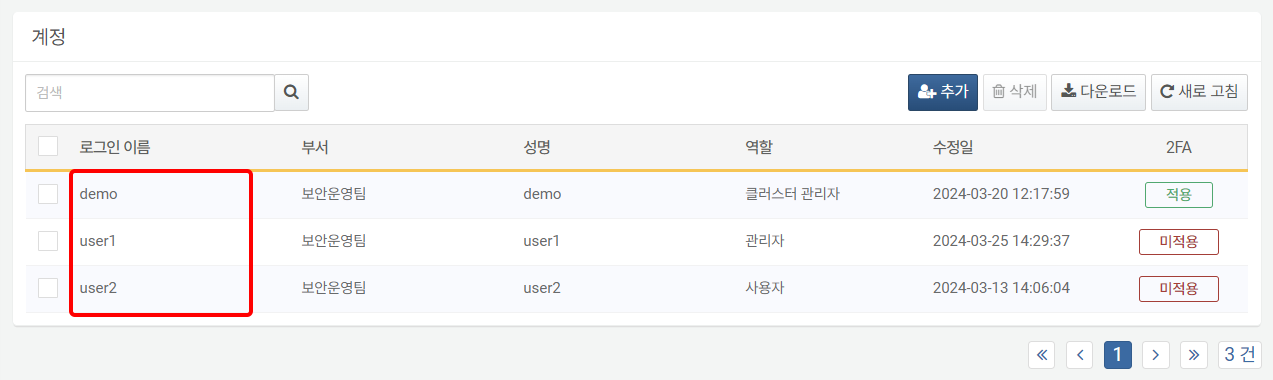


* **Tickets**: The ticket repositories that can be viewed with the account. By default, no tickets are selected. Only select the ticket repositories that you want to allow access to for the account.
* **Tables**: The tables that can be viewed with the account. By default, no tables are selected. Only select the tables that you want to allow access to for the account.

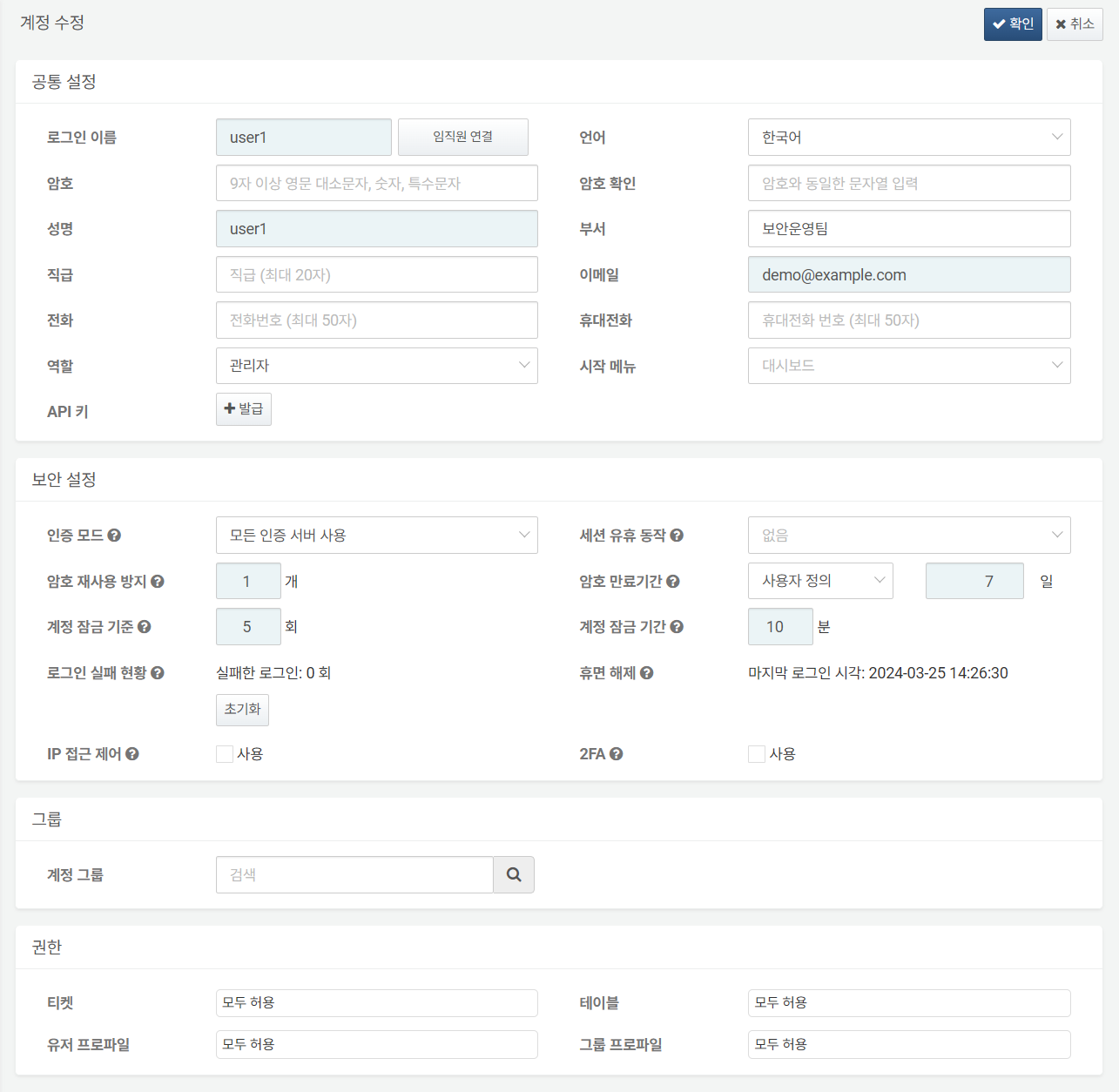
#### Modifying an Account

To modify properties such as the account's password or to unlock a locked account:

Click the **Login Name** of the account you wish to modify from the list.



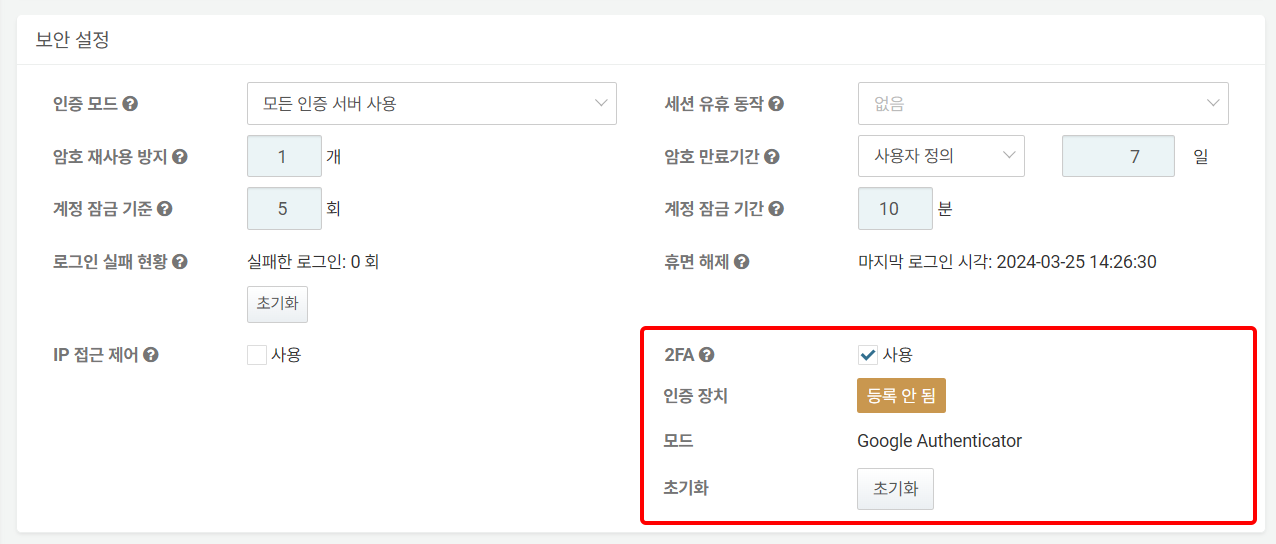
In the **Modify Account** screen, modify the information and click **Confirm**. For descriptions of the properties to be modified, refer to [Add Account](https://docs.logpresso.comnull).



The following content describes the tasks that can be performed in the account modification screen.

2FA Status Check/Reset

For accounts that previously had 2FA set up, the 2FA setup history can be checked in **Security Settings** as shown below. For information on how account users can set up their 2FA authentication devices and log in, refer to [here](https://docs.logpresso.comnull).



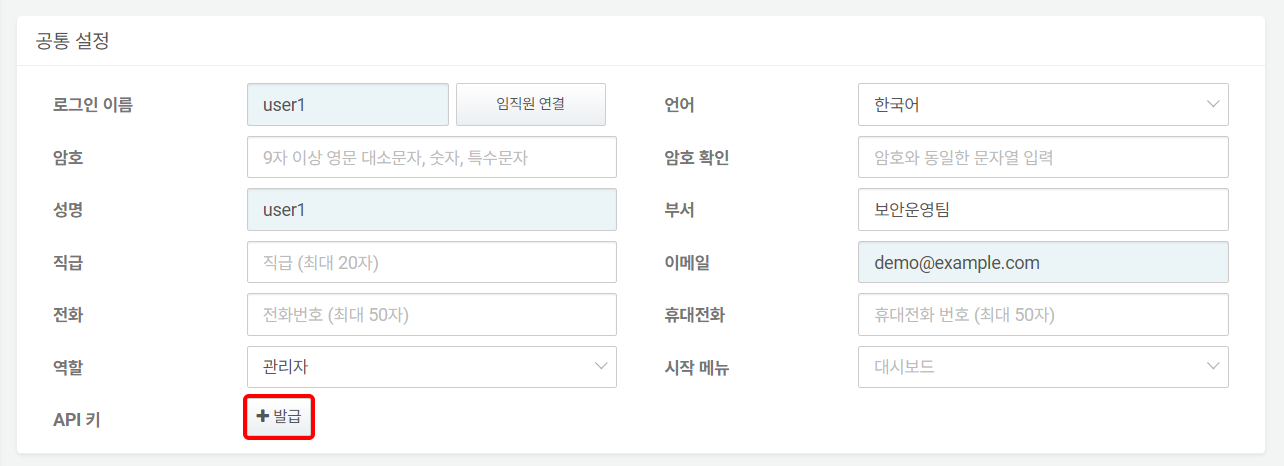
* **Authentication Device**: Indicates whether the 2FA authentication device is registered. If marked as **Not Registered**, it indicates that the account user has not yet set up 2FA. If the user attempts to log in in this state, they will be redirected to the 2FA setup screen.

: If marked as **Registered** (in green), it indicates that an authentication device is registered to the account, and the user is ready to authenticate using 2FA.

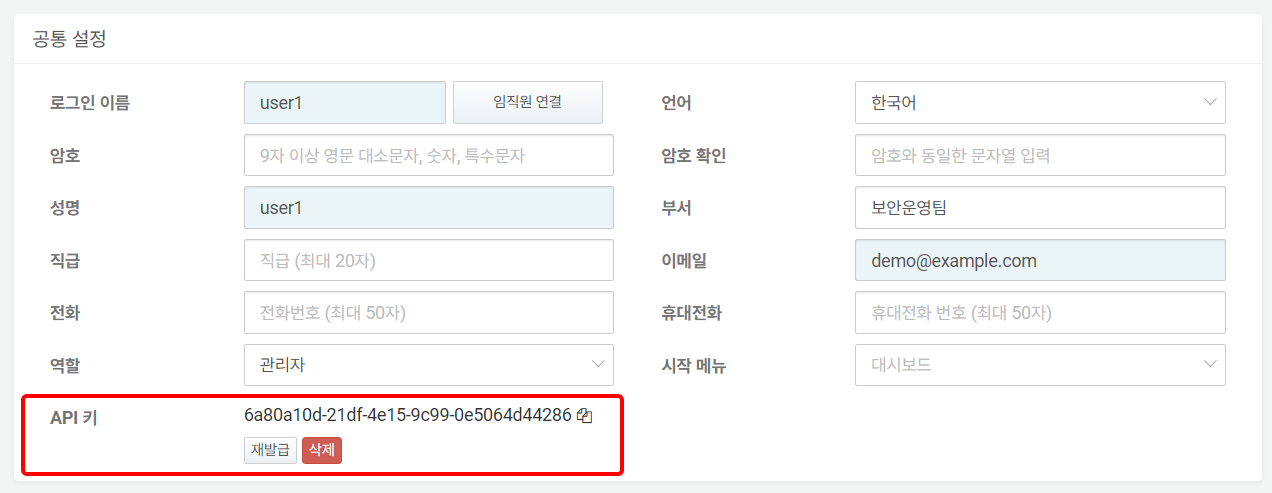
* **Reset**: If the account user has lost their 2FA authentication device or needs to change it, they can request a 2FA reset from the administrator on the login screen. The user's 2FA reset request will be sent to the email account registered with the administrator. To remove the 2FA authentication device information registered to the account, click **Reset**.

Issuing/Deleting API Keys

To use the Logpresso [REST API](https://docs.logpresso.comnull), an account and the API key issued to that account are required. To issue an API key, click **Issue** in the **API Key** section under **Common Settings**.



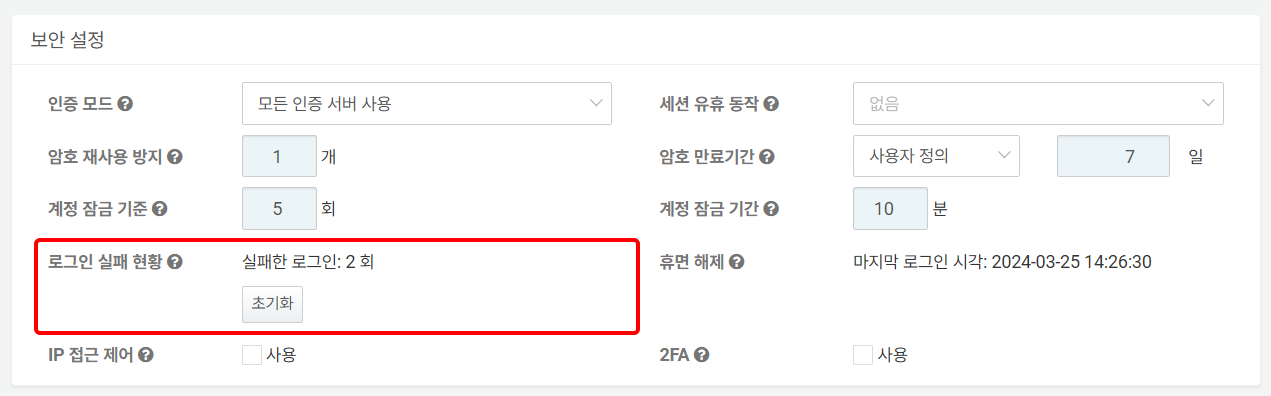
The following image is a screenshot of the screen where the API key has been generated.



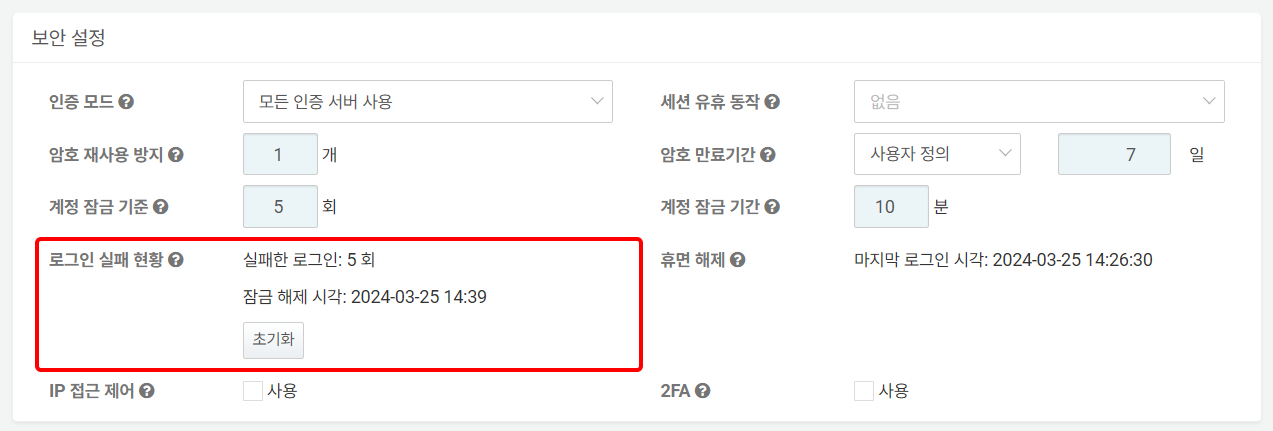
* **Copy to Clipboard**: Click the icon next to the generated API key to copy the API key to the clipboard.
* **Reissue**: Click to reissue the API key.
* **Delete**: Click to delete the issued API key.

Resetting Login Failures and Unlocking Accounts

If a user fails to log in consecutively, the number of failed login attempts will be displayed as shown in the following image.



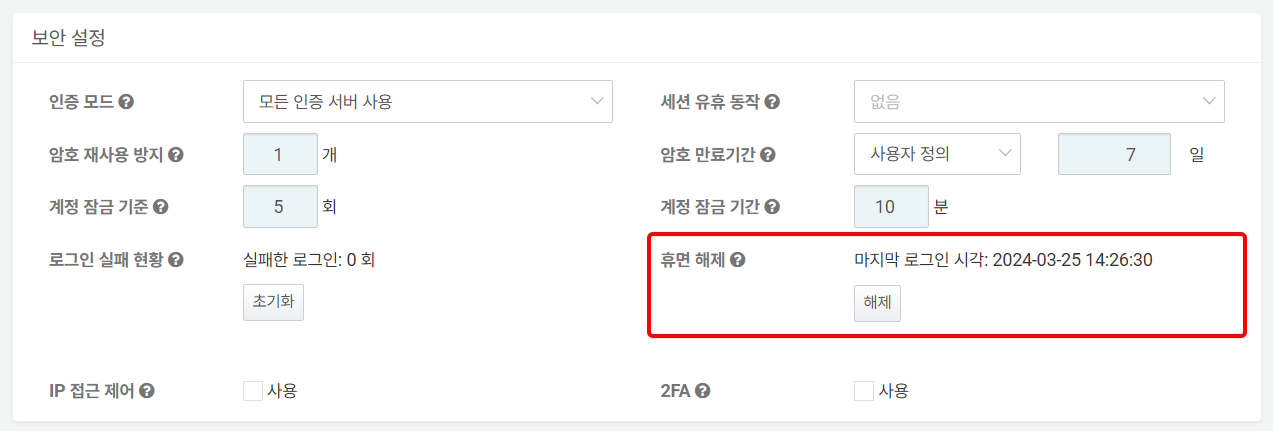
If the number of consecutive failures exceeds the account lock criteria, the unlock time will be displayed as shown in the following image.



To reset the number of login failures or unlock the account, click **Reset** in the **Login Failure Status** section.

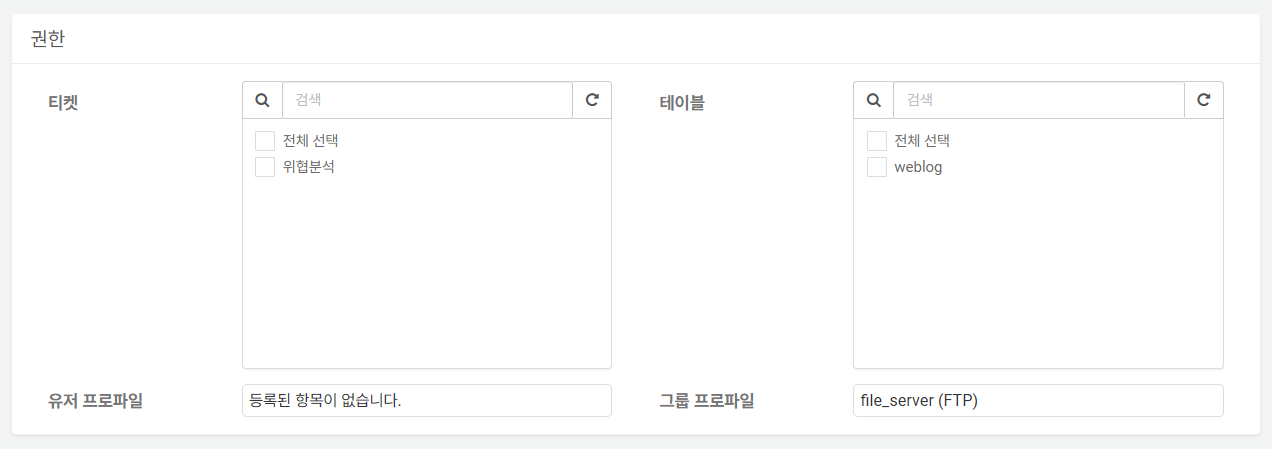
Reactivating Dormant Accounts

Depending on the server, accounts that have not logged in for a certain period may be set to transition to a dormant state. To reactivate a dormant account, click **Reactivate**.



Viewing/Changing Permissions

In addition to the ticket repositories and tables that the account user can access, you can check the connect profiles available to the account.



**Ticket** and **Table** permissions can be changed on this screen, but **User Profiles** and **Group Profiles** can be changed in the [Connect Profiles](https://docs.logpresso.comnull).

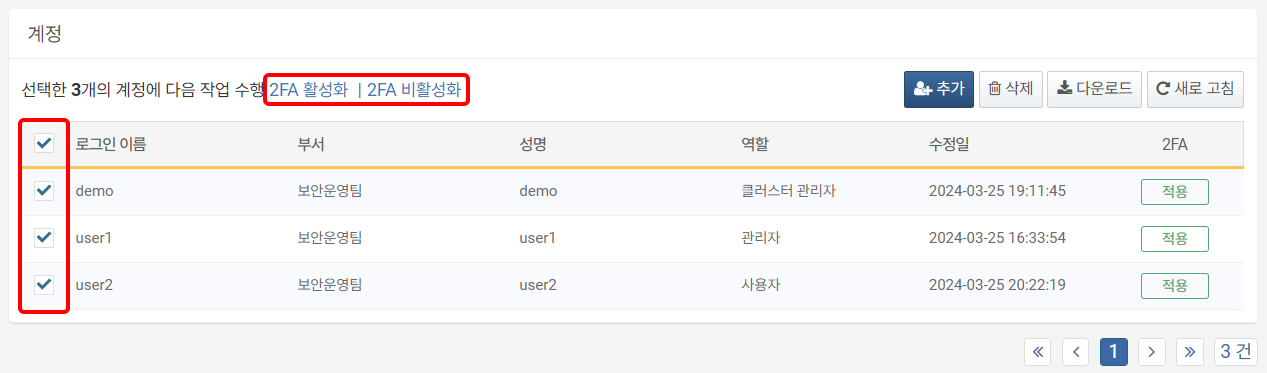
* **User Profile**: If the account is included in the account sharing settings of the connect profile, the name of that connect profile will be displayed in the list.
* **Group Profile**: If the account group to which the account belongs is included in the group sharing settings of the connect profile, the name of that connect profile will be displayed in the list.

#### Bulk Enable/Disable 2FA

To bulk enable or disable 2FA for one or more accounts:

Select the checkbox for the row containing the account information for which you want to enable or disable 2FA.

Click **Enable 2FA** or **Disable 2FA** in the toolbar.

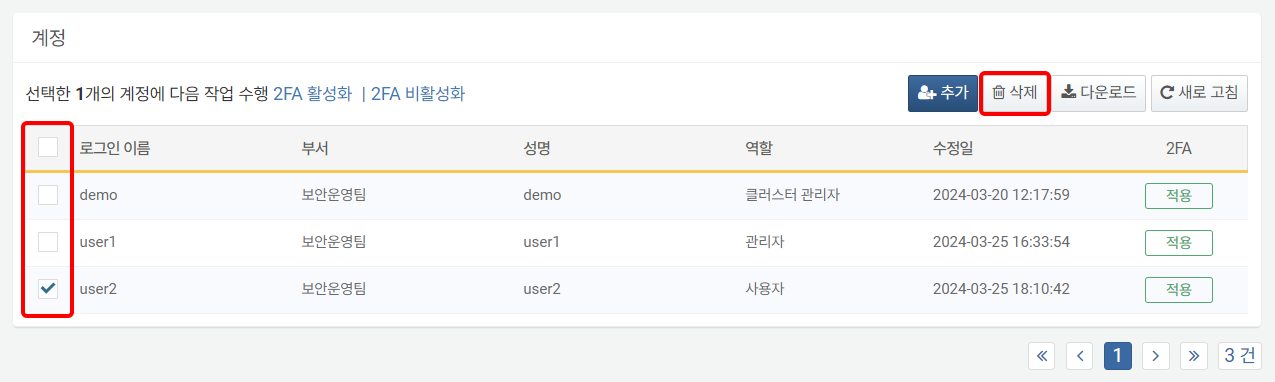


#### Deleting an Account

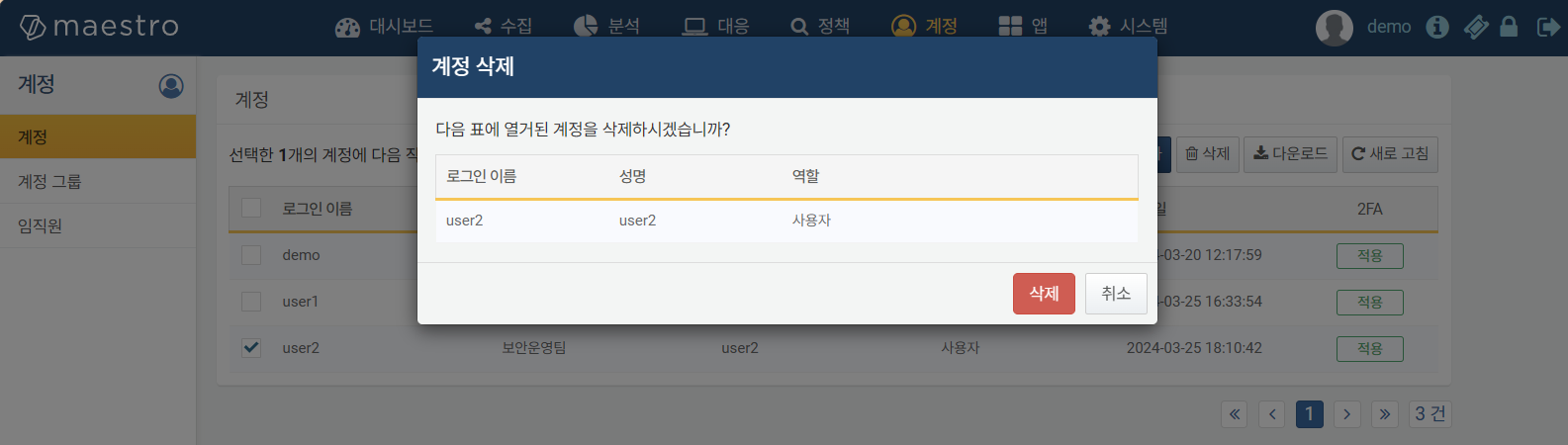
To delete an account:

Select the checkbox for the row containing the account information you wish to delete.

Click **Delete** in the toolbar.



In the **Delete Account** dialog, review the list of accounts to be deleted and click **Delete**. Click **Cancel** if you do not wish to delete.



When an account is deleted, only the account is removed, and other information related to the account remains intact. For example, if a ticket was assigned to the deleted account, the assignment history will remain.