### Log Schema

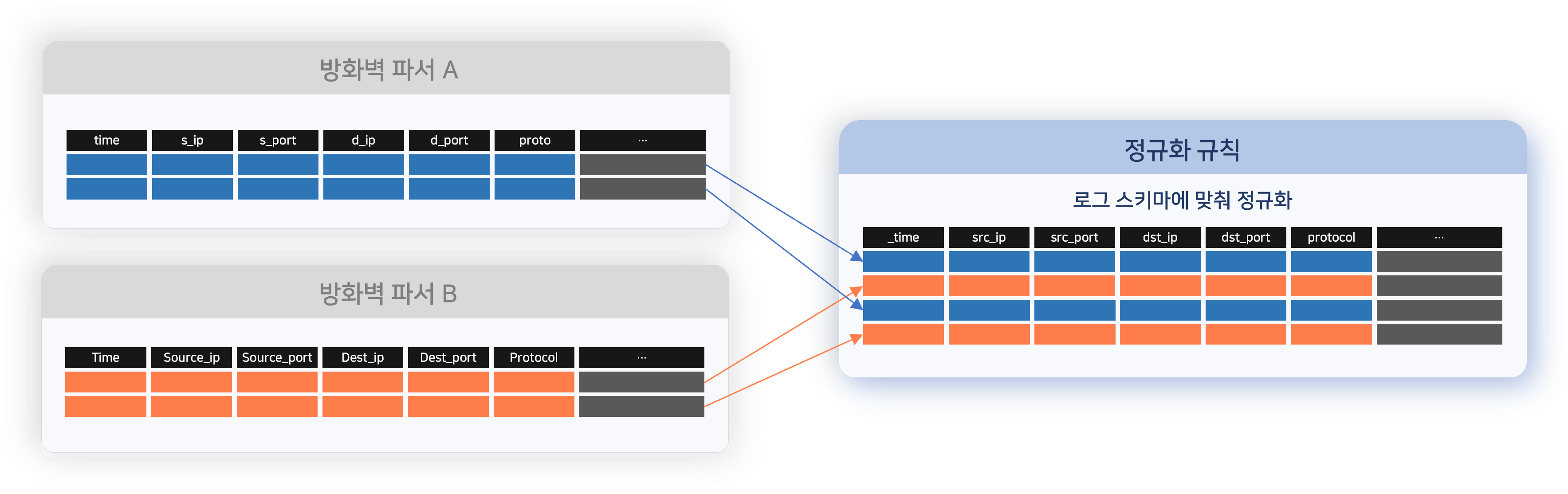
#### Overview

First, let us briefly examine the role of the parser. The parser extracts fields from input data on a record-by-record basis. For example, it identifies and extracts fields from the original logs of Palo Alto Networks firewalls and Fortinet FortiGate firewalls. However, the fields in the Palo Alto Networks firewall logs and Cisco Firepower firewall logs differ in name, structure, and order, making it difficult to compare or contrast them.

To utilize these logs effectively, the formats of different logs must be aligned. This is where the log schema becomes essential. The log schema performs functions similar to a database table schema, including:

* Standardizing the field names of input data identified by multiple parsers on a field-by-field basis.
* Defining the format necessary for restructuring and sorting fields according to usage.
* Assigning values extracted from the original records to empty fields if necessary.

The log schema serves as a reference when normalizing records according to the rules defined in the logger models. The following diagram illustrates the process of normalizing logs according to the log schema based on the normalization rules of the logger model.

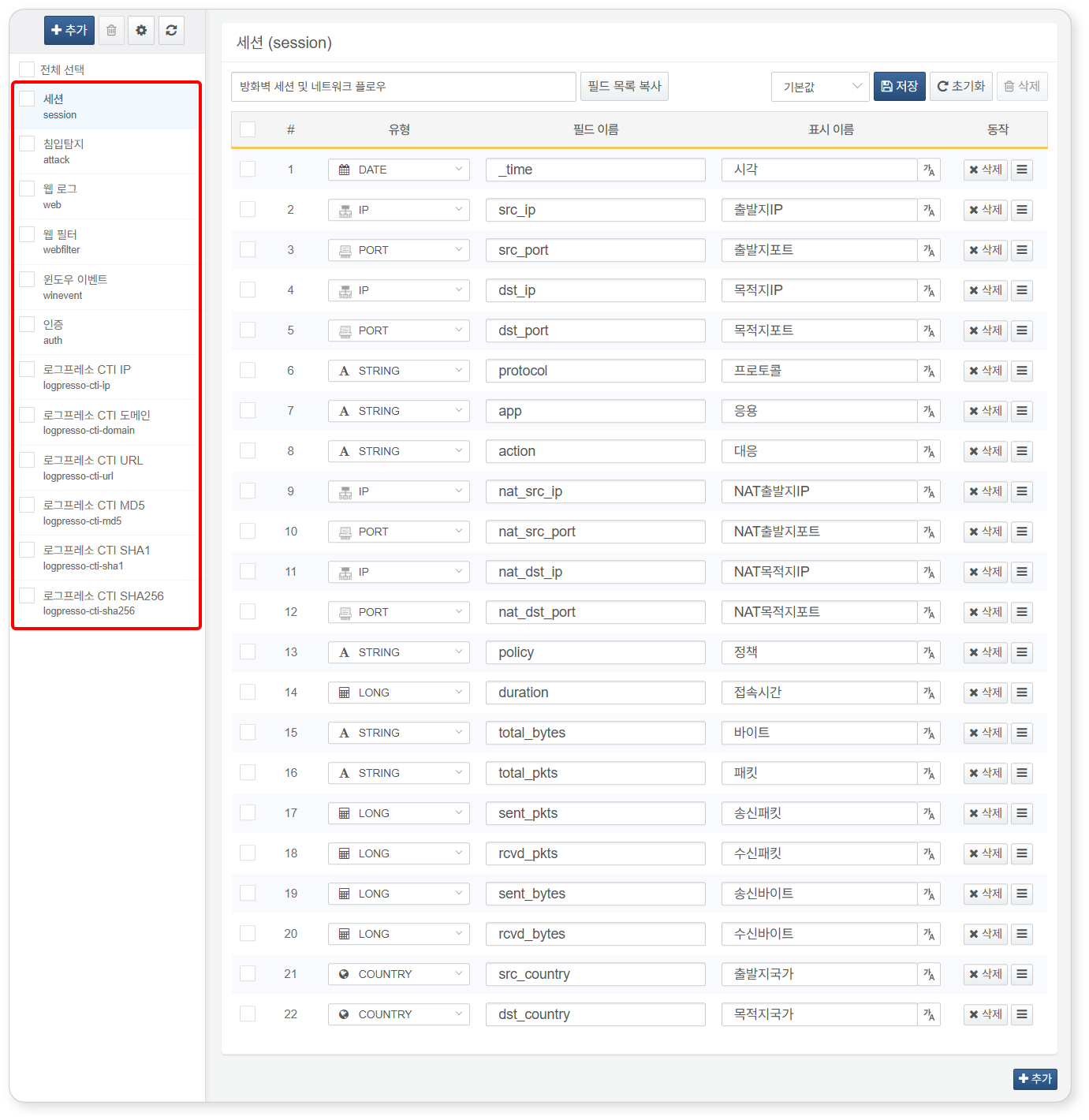


Base Schema and App Schema

Schemas can be categorized into base schemas and app schemas. Due to the nature of log schemas, which require the normalization of different heterogeneous logs, base schemas are used more frequently than app schemas.

**Base Schema**

This is a log schema provided by default to normalize general categories of heterogeneous logs. The red box area in the following figure shows the list of schemas that can be viewed when Logpresso Sonar is installed. The right area displays the list of fields defined in the log schema, specifically the field list of the session log schema.



The base schemas of Logpresso Sonar are as follows:

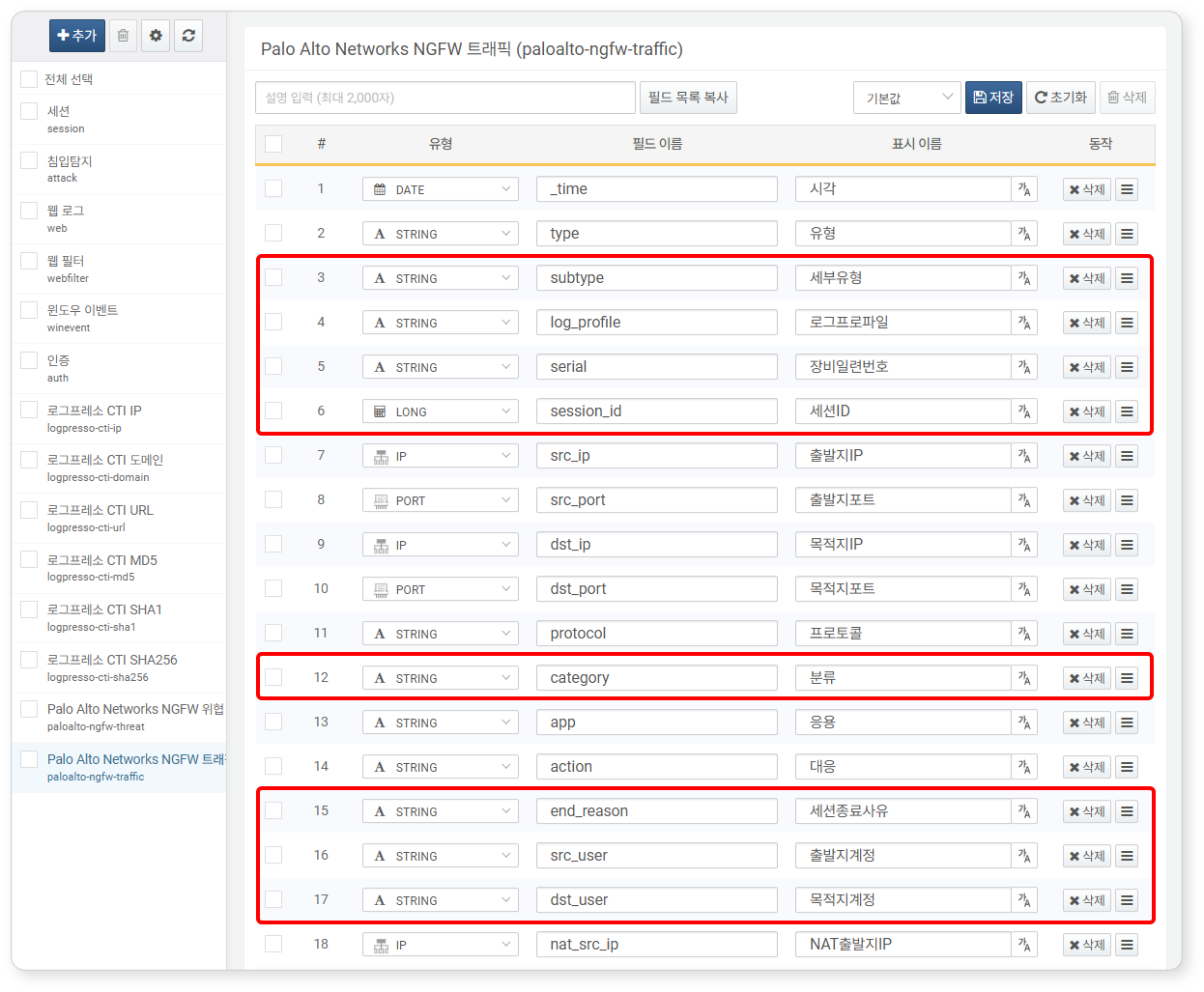
|  |  |  |
| --- | --- | --- |
| Name | Identifier (Schema Code) | Description |
| Session | session | Logs related to TCP/IP sessions |
| Intrusion Detection | attack | Logs from IPS and web firewalls for intrusion detection |
| Web Log | web | W3C standard web logs |
| Web Filter | webfilter | Logs from web proxies and harmful site blocking |
| Windows Event | winevent | Windows event logs |
| Authentication | auth | Logs related to remote logins such as Windows logon, SSH, VPN |
| Logpresso CTI IP | logpresso-cti-ip | Malicious IP addresses and related information from Logpresso CTI |
| Logpresso CTI Domain | logpresso-cti-domain | Malicious domains and related information from Logpresso CTI |
| Logpresso CTI URL | logpresso-cti-url | Malicious URLs and related information from Logpresso CTI |
| Logpresso CTI MD5 | logpresso-cti-md5 | Malicious file MD5 hashes and related information from Logpresso CTI |
| Logpresso CTI SHA1 | logpresso-cti-sha1 | Malicious file SHA-1 hashes and related information from Logpresso CTI |
| Logpresso CTI SHA256 | logpresso-cti-sha256 | Malicious file SHA-256 hashes and related information from Logpresso CTI |

Logpresso CTI can be utilized after registering an API key in the connect profiles.

**App Schema**

This log schema is provided alongside the installation of an app. Unlike the base schema, it can include unique fields from the source data for normalization.

The following figure shows a portion of the **Palo Alto Networks NGFW Traffic** log schema that can be viewed when the [Palo Alto Networks Firewall](https://logpresso.store/ko/apps/paloalto-ngfw) app is installed. The fields highlighted in red can be viewed when using the app schema, while they are omitted when querying logs with the base schema.



Utilization of Schema

**Logpresso Query Statements**

You can apply the log schema to input data using the [schema](https://docs.logpresso.comnull) command in query statements. The following is an example of applying the **Palo Alto Networks NGFW Threat** log schema (paloalto-ngfw-threat) to a processed sample of Palo Alto Networks firewall logs.

json "{}" | eval line="Apr 10 04:38:54 1,2012/04/10 04:38:54,012345678911,THREAT,spyware,1,2012/04/10 04:38:49,192.0.2.255,192.0.2.2,0.0.0.0,0.0.0.0,rule1,,crusher,web-browsing,vsys1,untrust,trust,ethernet1/2,ethernet1/1,forwardAll,2012/04/10 04:38:54,25466,1,80,59127,0,0,0x200000,tcp,drop-all-packets,\"habl.bin\",Trojan-Spy.Win32.Zbot.wti(12620),any,medium,server-to-client,0,0x0,United States,192.0.2.0-192.0.2.255,0," | parse overlay=t paloalto-ngfw | schema paloalto-ngfw-threat

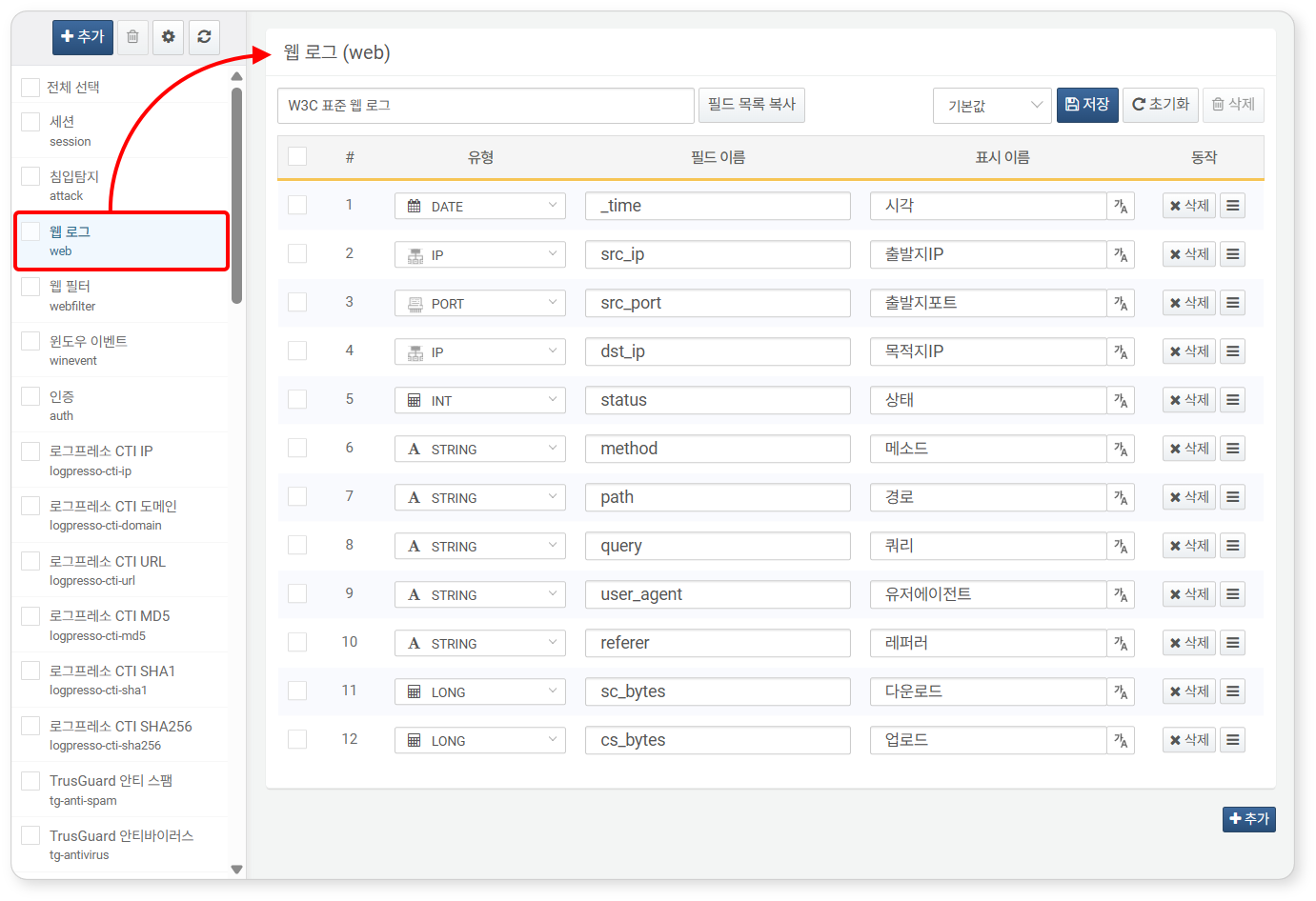
**Internationalization Support for Explanation Requests**

When an explanation is requested from employees suspected of security violations, an explanation request email is sent to the respective employee. In a multilingual environment, the supporting materials presented when employees [view explanation requests](https://docs.logpresso.comnull) or when primary reviewers [review explanations](https://docs.logpresso.comnull) need to be presented in the language used by the respective [employee](https://docs.logpresso.comnull). At this time, the display names defined in the log schema are utilized.

Internationalization of the log schema is supported from version 4.0.2404.0.

#### Viewing Log Schema

You can view the list of log schemas and the details of each log schema under **Collection > Log Schema**. The left panel displays the list of log schemas, showing the name and identifier of each schema. By clicking on a log schema in the list, you can check the list of fields defined in that log schema.



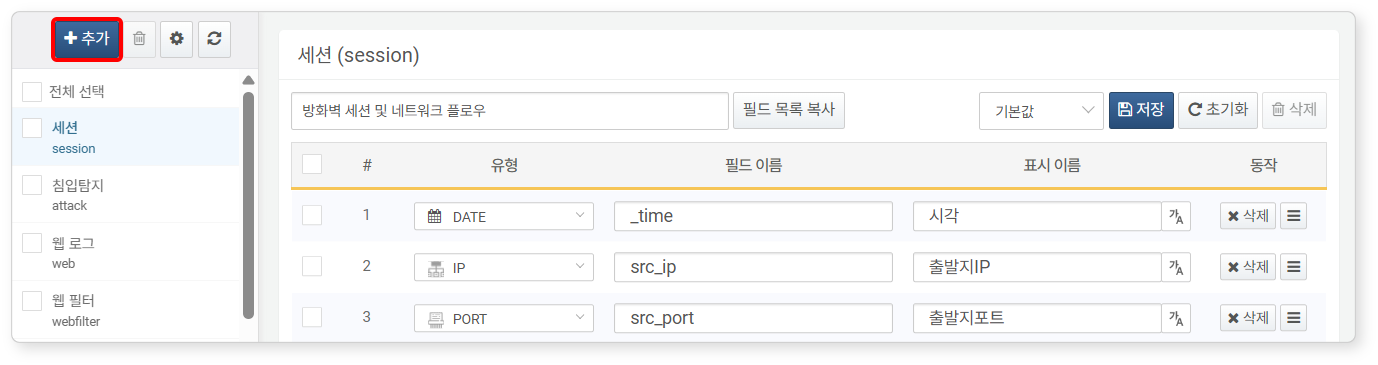
* **Order Number (#)**: The sorting order of the fields
* **Type**: The type of field value
* **Field Name**: The name of the field, consisting of letters, numbers, and underscores (\_)
* **Display Name**: The user-friendly name used in the web console
* **Action**: Handle for deleting or moving the field

Display names do not allow whitespace characters.

#### Adding Log Schema

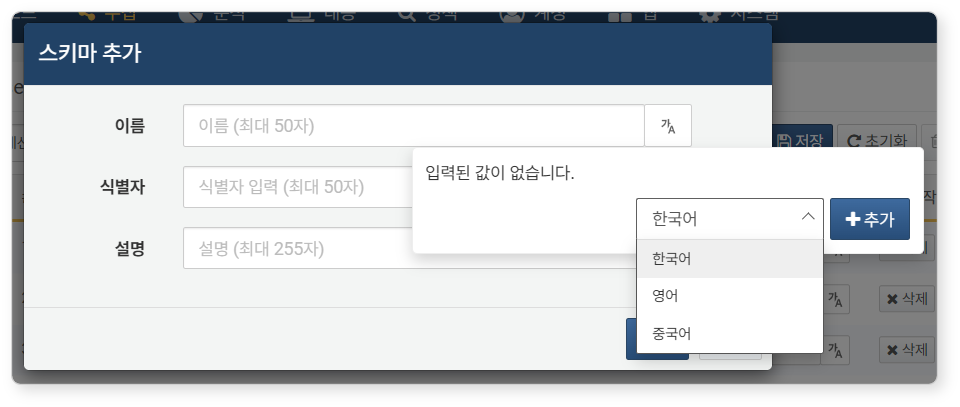
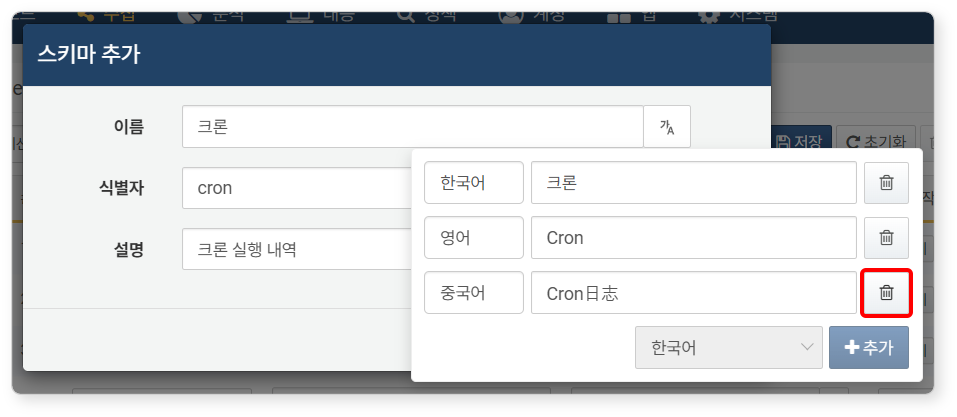
In most operational environments, using the base schema or app schema is sufficient. If normalization cannot be achieved with the base schema or app schema, you can add a custom log schema as follows:

Click **Add** above the log schema list in **Collection > Log Schema**.



In the **Add Schema** dialog, enter the schema properties.



* **Name**: The name of the log schema. The name entered here will be used as the default name in multilingual environments.
* To enter names for different languages in a multilingual environment, click the **가A** button on the right side of the input box.
* Select a language (Korean, English, Chinese) and enter the name corresponding to that language.
* 
* You can delete the added string by clicking the trash can icon on the right side of the string.
* 
* **Identifier**: A unique identifier used for schema calls in Logpresso query statements. The identifier is specified in the **\_schema** field at the time of log collection.
* **Description**: A description of the log schema displayed at the top of the log schema screen.

Once all settings are complete, click **OK**. Click **Cancel** if you do not wish to add the schema.

The added log schema will be empty without any fields. Refer to [Field Settings](https://docs.logpresso.comnull) to add fields to the schema and sort them.

#### Modifying Log Schema

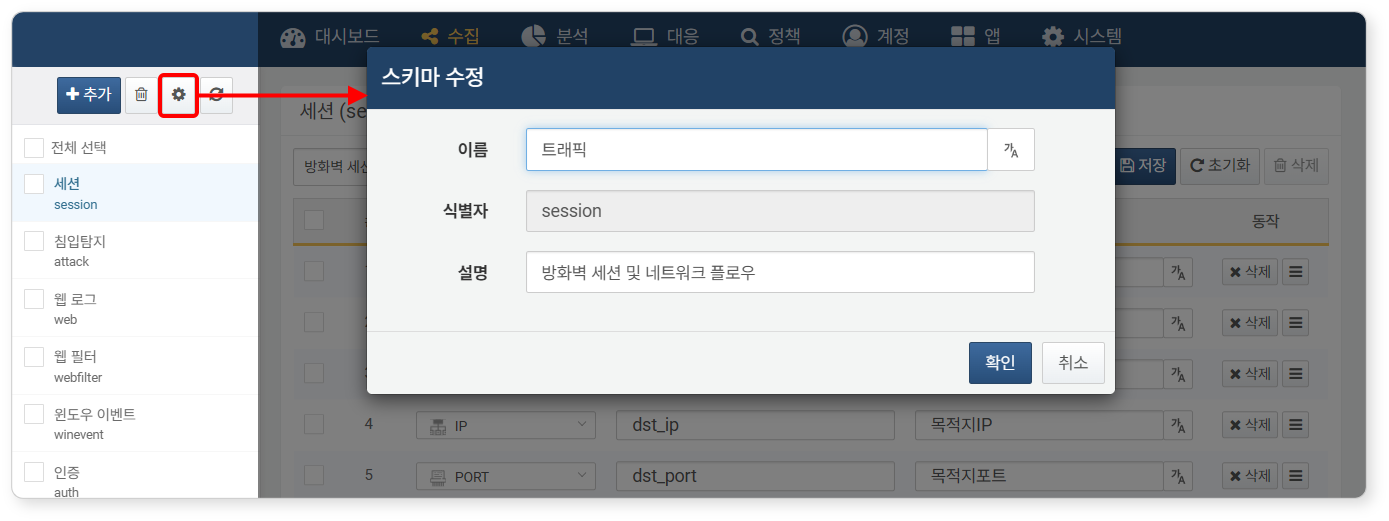
It is acceptable to add fields to the base/app schema as needed, but do not modify already defined fields, as this may cause issues with the operation of the logger models.

Changing Name/Description

To modify the name or description of a log schema:

Click the name of the schema you wish to modify in the log schema list under **Collection > Log Schema**, then click the gear button.

In the **Modify Schema** dialog, modify the name or description and click **OK**.

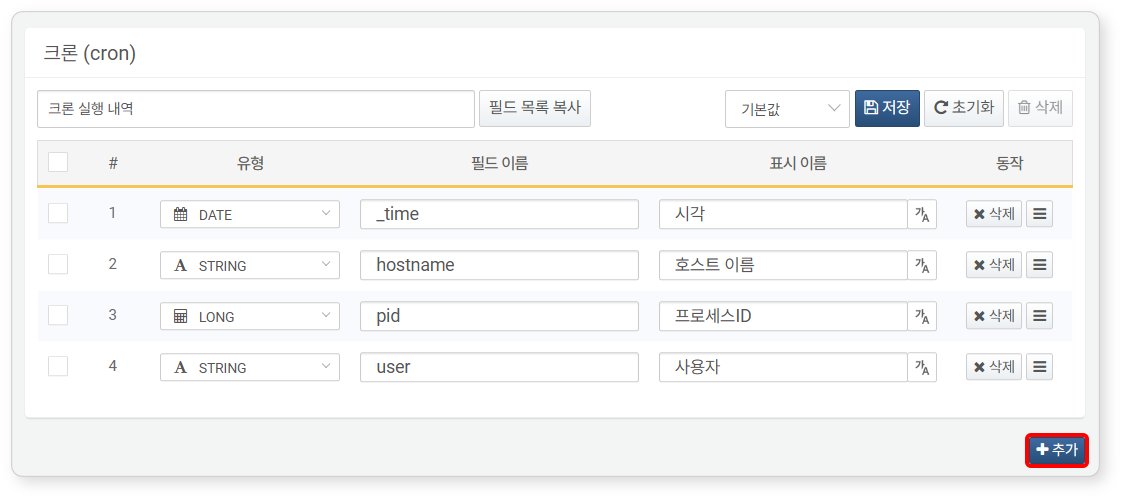


Field Settings

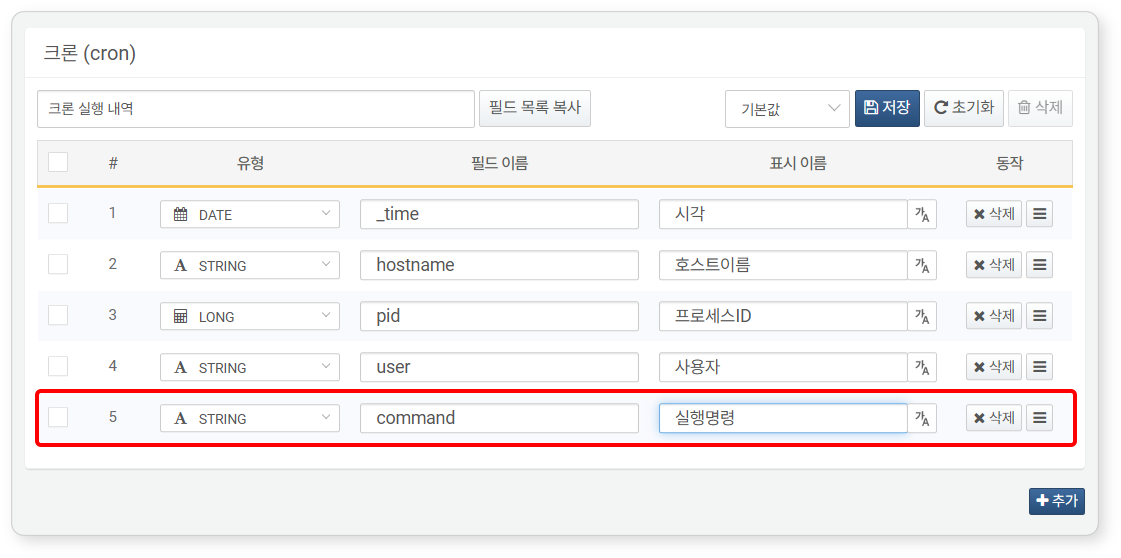
To add fields to the log schema or modify the properties of already defined fields:

Click the name of the schema you wish to modify in the log schema list under **Collection > Log Schema**. Here, we will use an arbitrarily added cron schema as an example.

Click **Add** in the lower right corner of the log schema screen to add fields.



Select/enter the **Type**, **Field Name**, and **Display Name** for the added field.

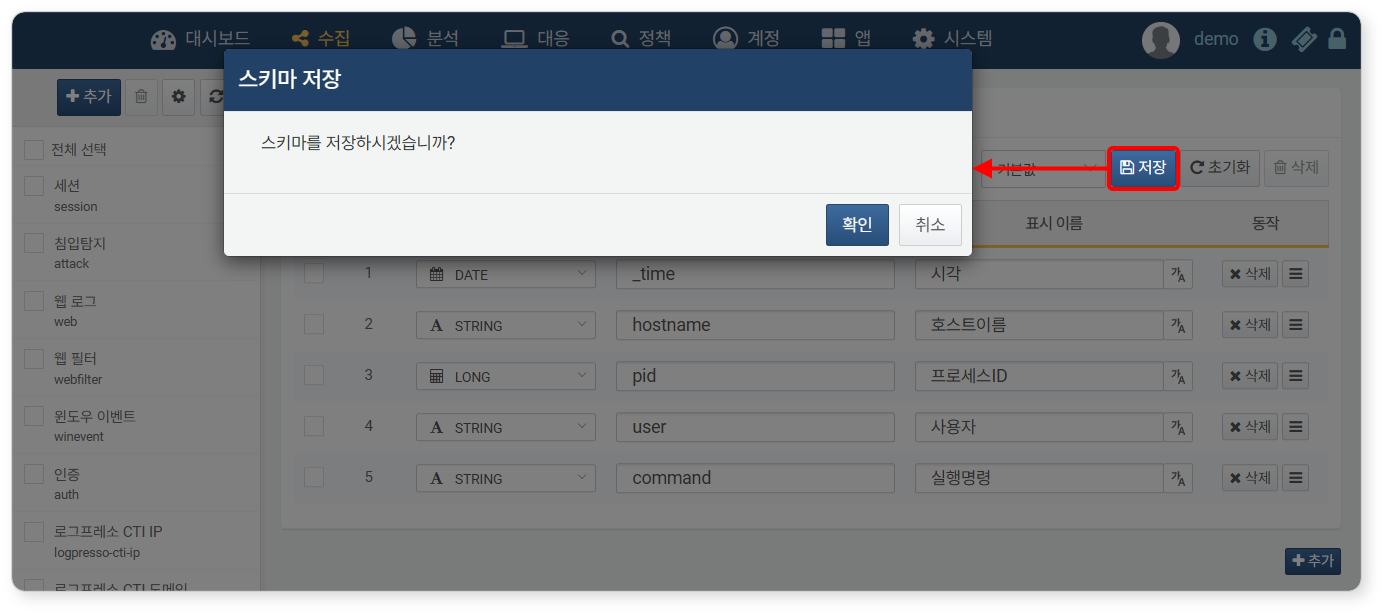


* **Order Number (#)**: The sorting order of the fields. This will increment sequentially each time a new field is added.
* **Type**: The type of field value. Choose one from the following:

|  |  |
| --- | --- |
| Type | Description |
| STRING | String |
| BOOL | Boolean value (true, false) |
| SHORT | 16-bit integer (-32,768 to 32,767) |
| INT | 32-bit integer (-2,147,483,648 to 2,147,483,647) |
| LONG | 64-bit integer (-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807) |
| DOUBLE | 64-bit floating point |
| DATE | Date/time with millisecond resolution |
| COUNTRY | ISO 3166-1 alpha-2 country code (e.g., KR) |
| PORT | Port number (0 to 65535) |
| IP | IPv4 or IPv6 address |
| MD5 | MD5 hash |
| SHA1 | SHA-1 hash |
| SHA256 | SHA-256 hash |
| URL | URL |
| DOMAIN | Domain address |
| BLOB | Binary data |

* **Field Name**: The name of the field, consisting of letters, numbers, and underscores (\_)
* **Display Name**: The user-friendly name used in the web console
* **Action**: Handle for deleting or moving the field
* You can click **Delete** to remove the field from the log schema. To delete multiple fields at once, check the checkboxes of the fields you wish to delete and then click **Delete** in the upper right corner of the log schema screen.
* You can change the order of fields by dragging the **Move Handle** to a different position.
* 

Once all field settings are complete, click **Save** in the upper right corner of the log schema screen, then click **OK** in the **Schema Save** dialog.



* Clicking **Reset** will revert to the last saved log schema.
* If you attempt to navigate away from the field settings without saving, the **Schema Save** dialog will appear.

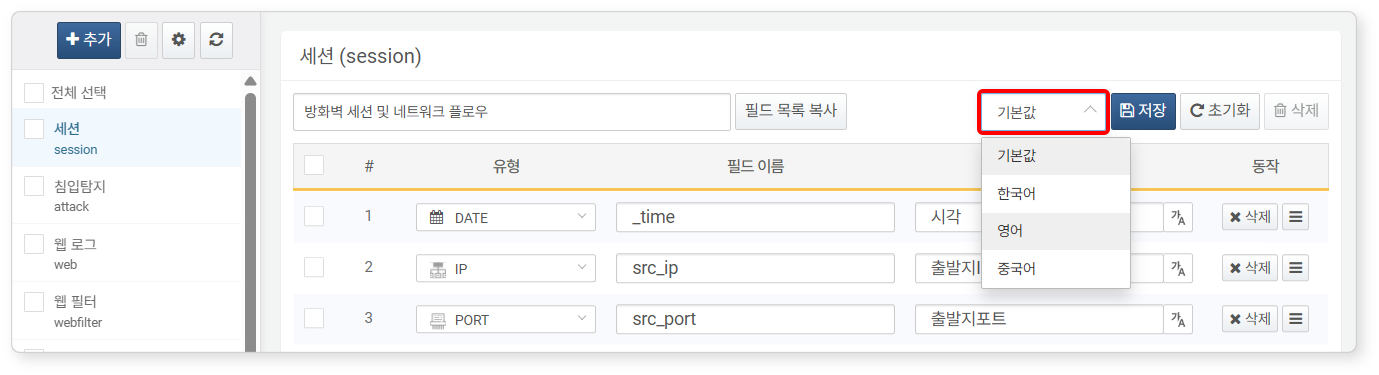
Internationalization Support

To support the internationalization of [explanation requests](https://docs.logpresso.comnull), you can set the log schema fields for each language.

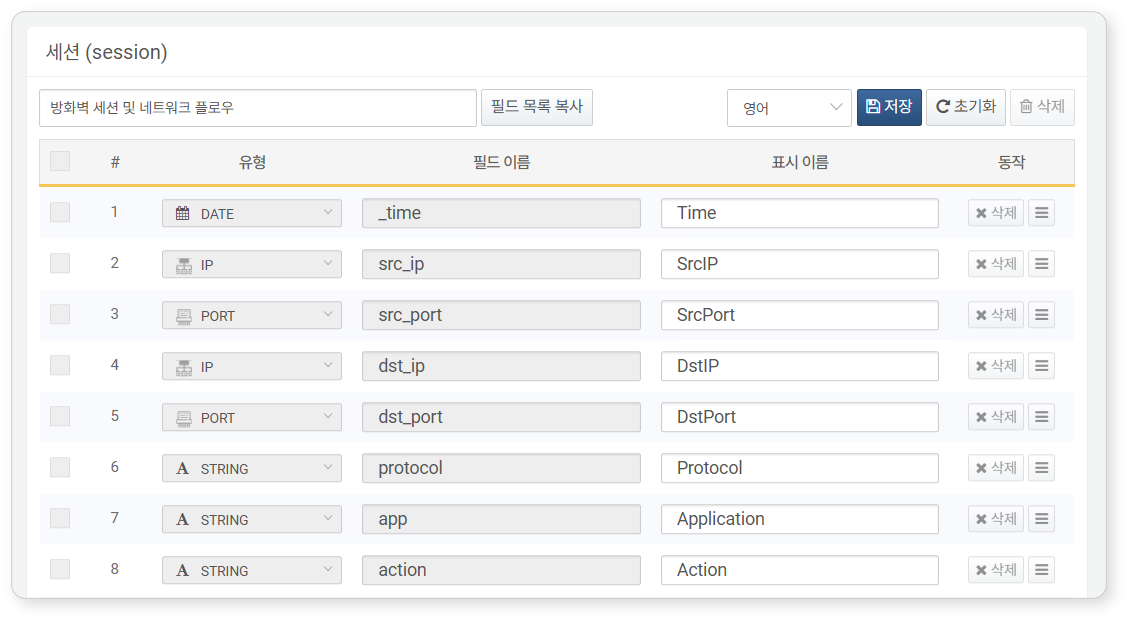
To set the display names of the log schema for different languages:

Click the name of the schema you wish to set internationalization for in the log schema list under **Collection > Log Schema**.

In the upper right corner of the log schema screen, select the language as shown in the following figure.



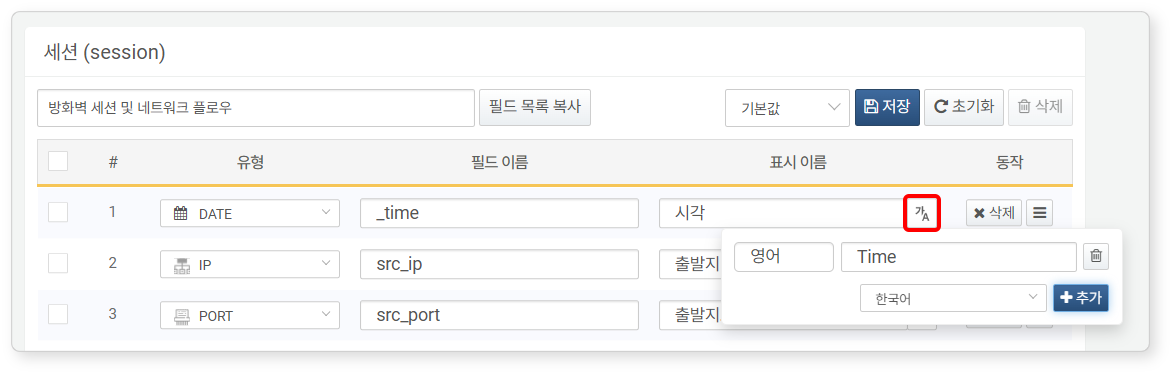
Enter the display name in the selected language.



After entering all display names, click **Save** in the upper right corner of the screen.

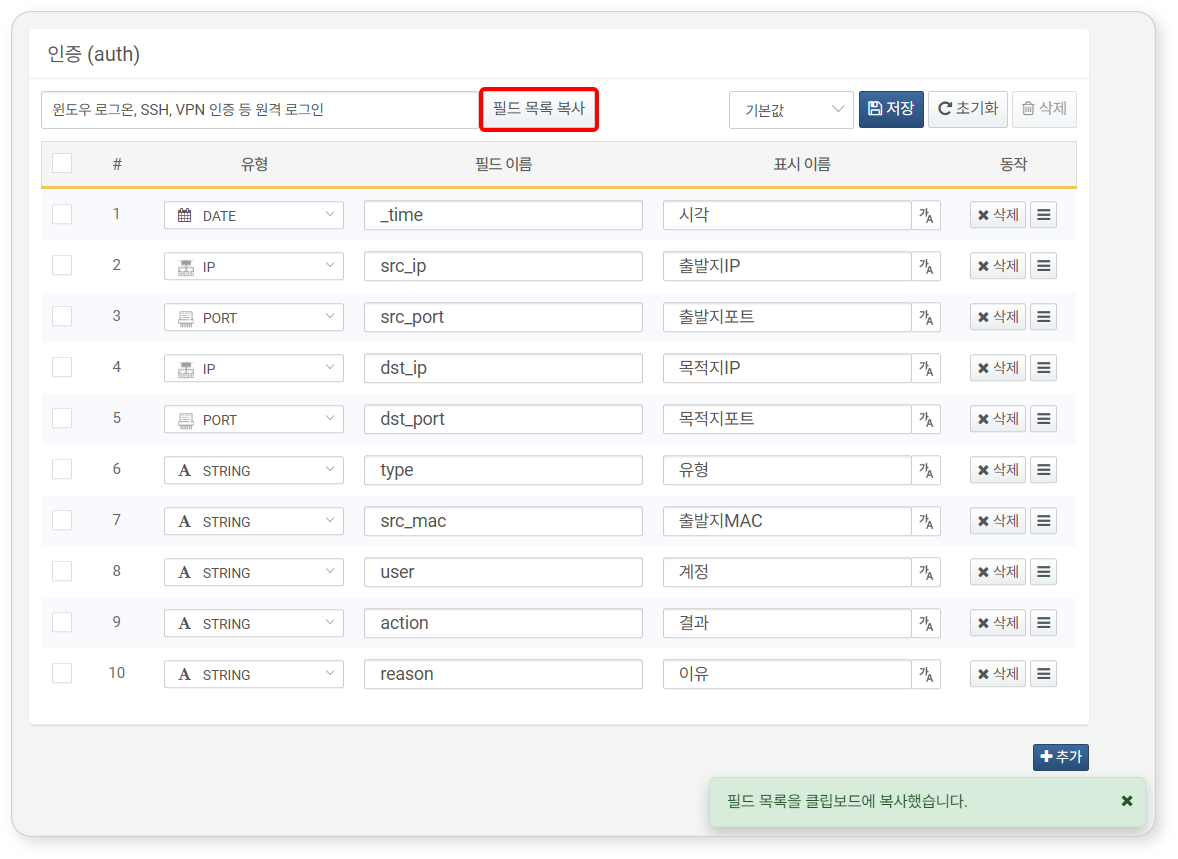
Click **OK** in the **Schema Save** dialog.

You can also set language-specific display names by clicking the **가A** button next to the **Display Name** of a specific field while the language is set to default.



#### Copying Field List

By clicking **Copy Field List**, the list of field names from the currently viewed log schema will be copied to the clipboard.



For example, if you copy the field list from the authentication (auth) schema view, it will be saved in the clipboard in the following format. You can utilize the copied field list when using query commands such as [fields](https://docs.logpresso.comnull) and [sort](https://docs.logpresso.comnull).

\_time, src\_ip, src\_port, dst\_ip, dst\_port, type, src\_mac, user, action, reason

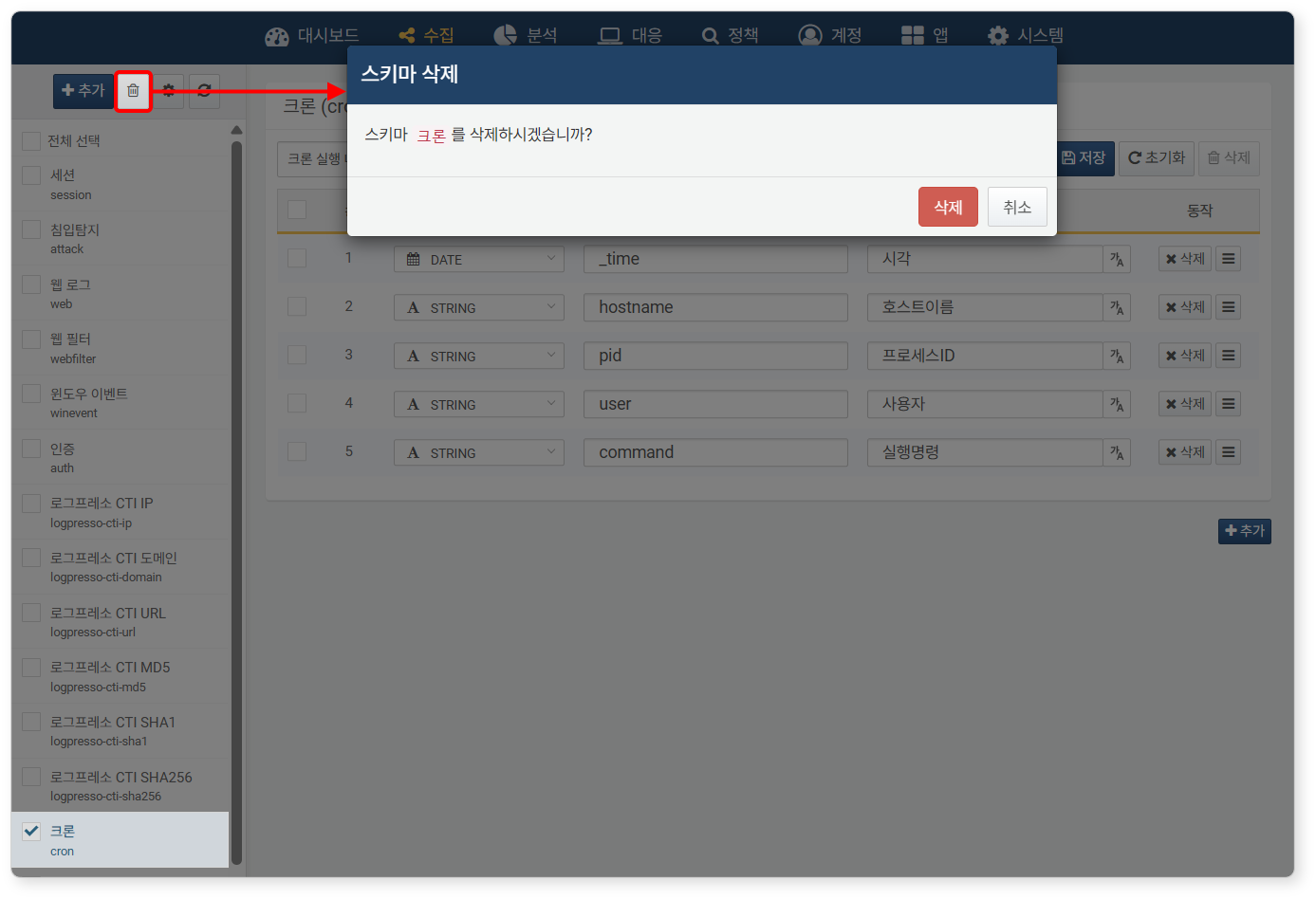
#### Deleting Log Schema

Do not arbitrarily delete base/app log schemas, as this may cause issues with the operation of the logger models.

To delete a log schema:

Click the checkbox next to the name of the schema you wish to delete in the log schema list under **Collection > Log Schema**, then click the trash can button.

In the **Delete Schema** dialog, modify the name or description and click **OK**.



If you are unable to delete the log schema, you can check the reason for the failure in the **Schema Deletion Failed** dialog.

