HDE
Liberation of Technology

HDE Controller

Web Server Manual

HDE, Inc.

Please note that this user manual may be subjected to change due to product upgrades without any prior notice.

HDE and HDE Controller is a registered trademark of HDE, Inc.

All group names and product names listed in this manual are registered trademarks to each of the groups and products respectively.

This manual may only be copied by printing in PDF format. Any other forms of copying, transferring, loaning, adapting, translating, or public distribution of this manual is not allowed.

Reprinting or reproducing this manual without HDE's permission is strictly forbidden.

© 2011 HDE, Inc.

How to Read this Manual

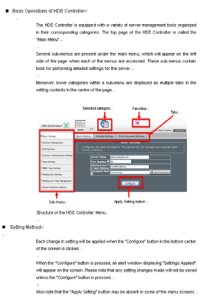
About this Manual

The “HDE Controller Installation Manual” provides users with instructions to installing OS and the HDE Controller (this Product) as well as steps for configuring the initial settings of the Product.

Annotations are provided for any matters requiring special attention and phrase supplements.

	Any matters which require special attention are marked with this "Alert" icon in bold frame.

	Contents which provide useful reference for using HDE Controller are marked with this "Hint" icon.



HDE Controller X

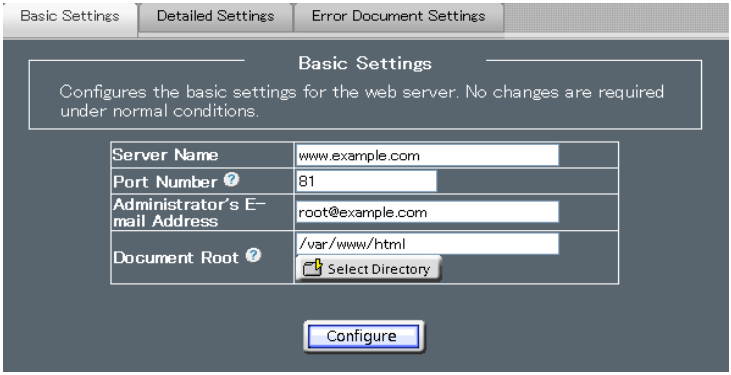
Web Server

1. Basic Settings

Configure the basic settings of the Web Server.

■ Basic Settings

Enter the appropriate "Server Name", "Port Number", "Administrator's E-mail Address", and “Document Root" in the corresponding fields.



- Server Name

  Enter the public server name (Set as www.example.com as an example).

- Port Number

  Typically, port number 80 is used. When changing the port number, users are required to specify the port number after the server name of the URL string. (For example, http://www.example.com:80/).

- Administrator’s E-mail Address

  Enter the Web administrator's E-mail address in this field as the administrator's E-mail address. Often times, address such as "webmaster@example.com" is entered here instead of the personal e-mail address of the admin (these address will eventually be used to enable the administrator to receive e-mails that are transferred via mail server settings and mailing lists).

- Document Root

Specify the directory which you wish to release to the public as the Web server.

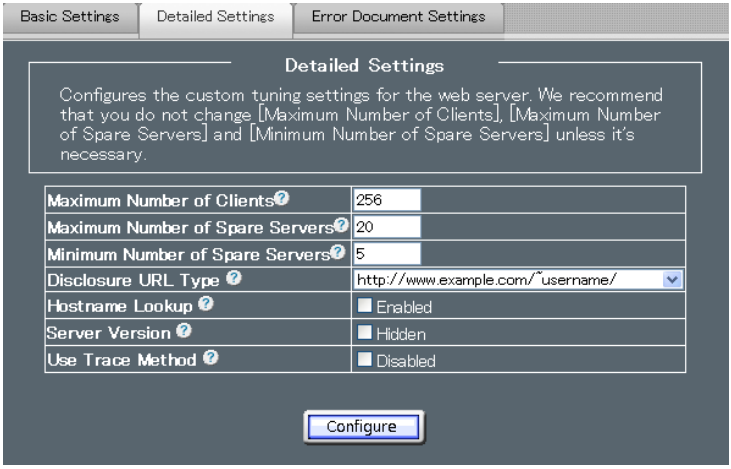
Users may enable file upload via FTP by creating a directory under the home directory of the user who manages the document root and setting such directory as the document root.

> ⚠ Users are not required to make any changes to the "Port Number" and "Document Root" under normal conditions; however, if the website administrator and the server administrator is not the same user, it might be convenient to set the document root to the home directory of the Website administrator.

Click the “Configure” button to complete your settings.

■ Detailed Settings

Configures the custom tuning settings for the web server such as maximum number of clients, spare servers as well as the URL type used when disclosing the user range to the public.



- Maximum Number of Clients

  Specify the maximum number of simultaneous connections from clients. Increasing the maximum number of simultaneous connections will allow more connections, but require higher amount of resources. The default value is 256 and the maximum value is 1024.

- Maximum Number of Spare Servers

  Specifies the maximum number of server processes during idle state. The default value is 20.

- Minimum Number of Spare Servers

  Specifies the minimum number of server processes during idle state. The default value is 5.

- Disclosure URL Type

  Enter in either of the following format.

  Ex.

  http://example.com/~username/

  http://example.com/users/username/

  Click the "Configure" button to finish configuration if your settings are correct.

- Hostname Lookup

  Configure HostnameLookup. When looking up hostnames, the remote hosts will be displayed on the access log by hostnames. Please note that the performance of the Web server may decrease when performing lookup.

- Server Version

  Check the “Hidden” box if you do not wish to show the server version on server response headers and error messages, etc. Uncheck this box if you wish to release information regarding the server version.

- Use Trance Method

  Check the "Disable" box if you wish to disable the use of trace method of HTTP. Check the box if you wish to enable the use of Trace method.

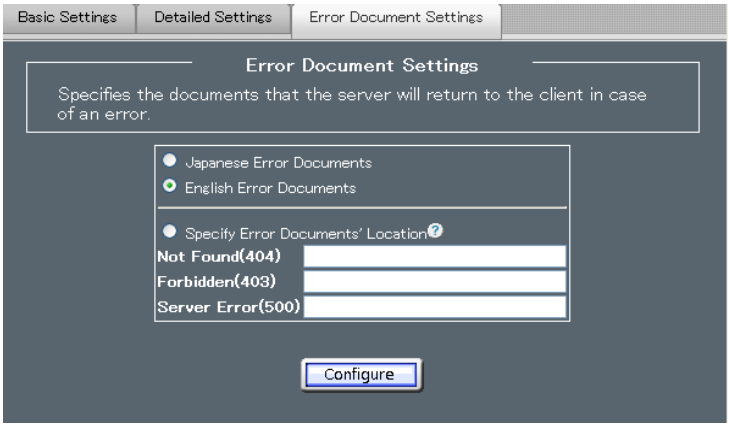
  We recommend users to disable the use of Trace method unless necessary as there are methods such as cross-site tracing which uses the trace method to perform harmful attacks on servers.

  This setting will only be displayed if your Apache version is above 2.0.55.

■ Error Document Settings

Configure the error document sent to the clients when the requested Website address is incorrect.



Select the language of the error documents from below:

- Japanese Error Documents
- English Error Documents

If you wish to specify a location were the files containing the error message are saved, please select "Specify Error Documents' Location" and enter the path of the files in each of the corresponding fields.

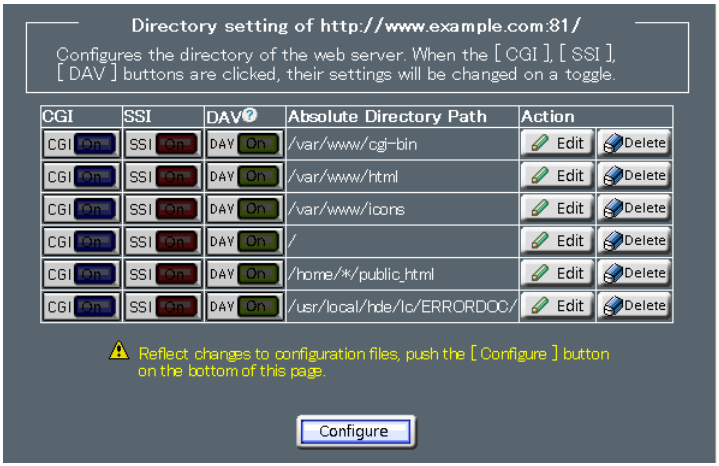
- Not Found (404)
- Forbidden (403)
- Server Error (500)

If your configurations are correct, click the "Configure" button to finish the settings.

2. Directory Management

Configure the CGI, SSI, DAV, and access control of the directories created in the "Add Directory" Menu. Users may also choose to delete specific directories from this screen.

Click on "Directory Management" to show the directories configured with CGI, SSI, DAV, and access control.

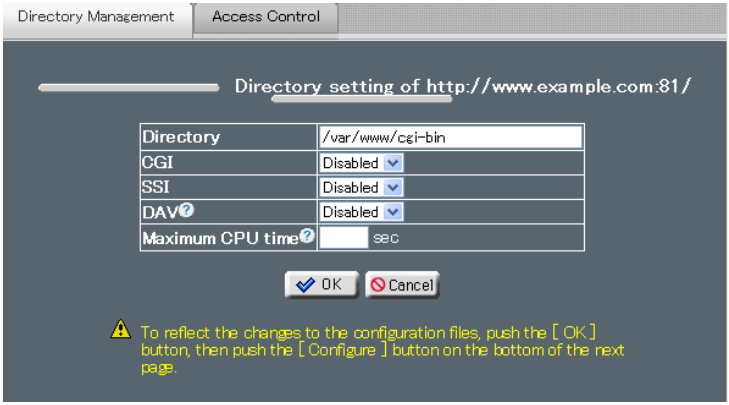


You may change the permission (ON/OFF) status of CGI, SSI, and DAV by clicking on the buttons located on the left side of the changed directory.

After configuring the settings for CGI, SSI, and DAV, click the "Configure" button to apply your configuration changes.

Click the "Edit" button to change the configured directory or the access control of the directory.

■ Directory Basic Settings



To change the directory settings, change the directory name on this screen and configure its CGI, SSI, and DAV if necessary.

To restrict the CPU usage time for CGI and SSI, enter the amount of time in the "Maximum CPU time" field in seconds. The time configured in this field represents the actual amount of time the CPU is used by CGI; it is not the time counted up from the time of boot.

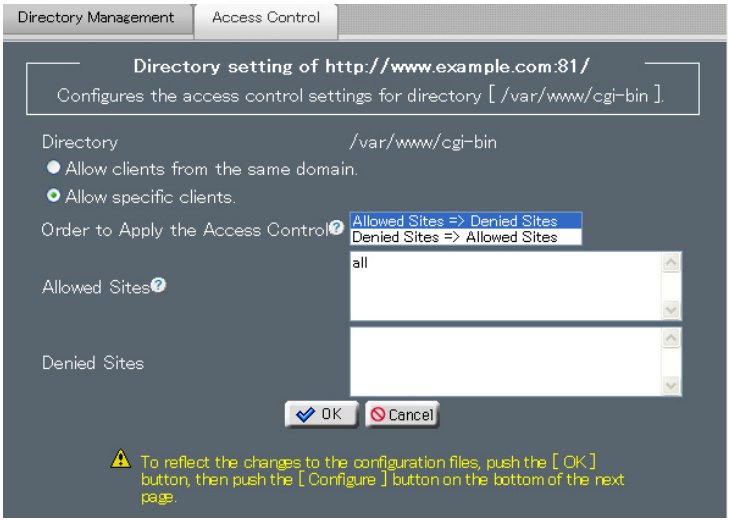
No restriction will be set if this field is omitted.

If you have completed your configurations, click the "OK" button to proceed to the next screen and click the "Configure" button to finish the configuration.

■ Access Control

Configure the access control of directories.

To access this screen, click on the "Edit" button on a directory from the directory list to bring up the "Directory Settings" screen; then click the "Access Control" tab on top to switch your screen.



Select "Allow clients from the same domain" if you wish to only allow access from clients belonging to the same domain.

Select "Allow specific clients" if you wish to specify which clients to grant access.

Select the order to apply the access control rules from the "Order to Apply the Access Control" field.

By setting [Allow => Deny], Sites Allowed will be evaluated before Sites Denied. This is useful for denying connections from specific sites. Access is denied by default.

By setting [Deny => Allow], Sites Denied will be evaluated before Sites Allowed. This is useful for allowing certain access from specific sites. Access is allowed by default.

Enter each allowed sites and denied sites in the corresponding text fields in the appropriate format.

If your configurations are correct, click on the "OK" button.

Return to the directory list screen and click on "Configure" to complete your configurations.

Text format allowed to be inputted in the Access Control fields.

Hostname	host.example.com
IP Address	192.168.0.1
Part of an IP Address	192.168.0.
IP Address/Netmask	192.168.0.0/255.255.255.0
Multiple Entries	192.168.0.0./24 172.16.0.0/16 （separate each entries with space or new line）.
Specify All	All (applies settings to all hosts).
Domain Name	.example.com

3. Add Directory

Add directories to be released to the public on the Web server and configures CGI, SSI, DAV permission settings.

- Directory

  Enter the path of the directory to be added or click the "Select Directory" button to select the directory from the directory selection screen.

- CGI

  Select to enable or disable CGI for this directory. CGI will not function if "Disabled" is select.

- SSI

  Select to enable or disable SSI for this directory. SSI will not function if "Disabled" is select.

- DAV

  Select to enable or disable DAV for this directory. DAV will not function if "Disabled" is select.

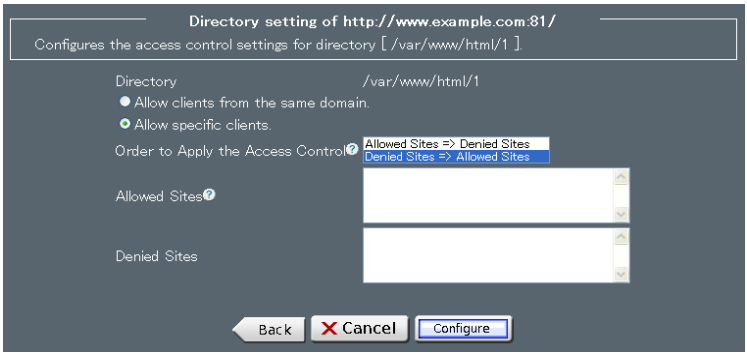
- Maximum CPU Use Time

  To restrict the CPU usage time for CGI and SSI, enter the amount of time in the "Maximum CPU time" field in seconds. The time configured in this field represents the actual amount of time the CPU is used by CGI; it is not the time counted up from the time of boot.

Click the "Next" button to proceed to the next setting.

■ Directory Access Control

Configure access control settings for directories.



Select "Allow clients from the same domain" if you wish to only allow access from clients belonging to the same domain.

Select "Allow specific clients" if you wish to specify which clients to grant access.

Select the order to apply the access control rules from the "Order to Apply the Access Control" field.

By setting [Allow => Deny], Sites Allowed will be evaluated before Sites Denied. This is useful for denying connections from specific sites. Access is denied by default.

By setting [Deny => Allow], Sites Denied will be evaluated before Sites Allowed. This is useful for allowing certain access from specific sites. Access is allowed by default.

Enter each allowed sites and denied sites in the corresponding text fields in the appropriate format.

Text format allowed to be inputted in the Access Control fields.

Hostname	host.example.com
IP Address	192.168.0.1
Part of an IP Address	192.168.0.
IP Address/Netmask	192.168.0.0/255.255.255.0
Multiple Entries	192.168.0.0./24 172.16.0.0/16 (separate each entries with space or new line).
Specify All	All (applies settings to all hosts).
Domain Name	.example.com

If you configurations are correct, click on the "Configure" button to complete your configurations.

4. Directory Authentication Settings

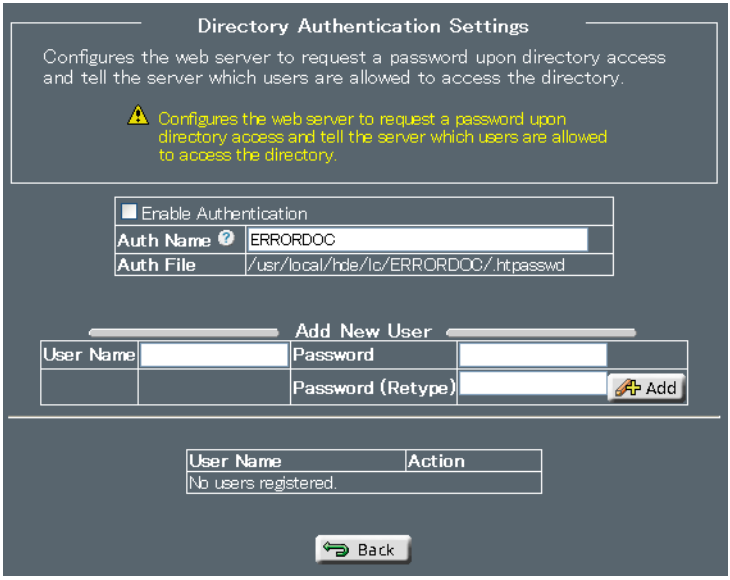
Configure the authentication settings for the directories in the "Add Directory" Menu to be released to the public on the Web server.

■ Directory Authentication Settings

Click on the "Edit" button of the directory you wish to configure authentication settings on from the Web directory list.

The screen containing the authentication content will be displayed.

Please follow the instructions on screen and enter the required items.



- Enable Authentication

  Check the box beside “Enable Authentication”.

- Auth Name

  Enter the content to be displayed upon authentication in the "Auth Name" field. (Ex. ENTERID/PASSWORD).

- Add New User

  Create a new user.

  For this example, we will enter the following.

Username	example
Password	test

  Users will be asked to enter their password twice for confirmation.

  The new user will be added to the list when the "Add" button is pressed after all necessary information has been entered.

You may choose to add additional users by specifying the username and password for each new user.

Click on the "Back" button after you have completed adding the necessary number of users you need.

Return to the directory list screen.

A list of registered users will be displayed on for each directory. Please confirm that the icon on the left side is set as "Authentication Enabled".

If your configurations are correct, click on the "Configure" button to complete your configurations.

- How to confirm authentication from browser

  Access the directory have set authentication on from your browser and confirm that the directory has authentication configured and that you can pass the authentication with the specified username and password.

Changing the authentication state of the directory

This section will explain how to disable or change the authentication state of a directory.

To disable authentication on a directory, click on the folder icon on the left side of the directory path in the directory list.

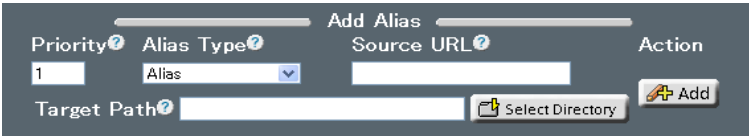
Clicking on the folder icon of a directory which has authentication enabled will disable the authentication and vise versa.

To add a new authorized user, click the "Edit" button of the directory and add users in the same way as when you have set the directory authentication.

5. Alias Settings

Add Alias used for converting addresses for Web server accesses.

■ Add Alias



● Priority

Priority indicates the position of where a new alias will be inserted to. If there is a pre-existing alias in the specified position value, the specified position will be overwritten by the new alias and the pre-existing alias will be moved down the list by 1 position value.

● Alias Type

For alias type, select one of Alias, AliasMatch, ScriptAlias, or ScriptAliasMatch from the following directive.

Alias	Assign the particular patterns of the URL to the corresponding files/directories. Patterns matching for the Source URL will be replaced by the Target Path directly.
AliasMatch	Similar to Alias except users may use regular expressions for the Source URL as well as the back references such as $1, $2.... for the Target URL.
ScriptAlias	Specify the values in ways similar to that of Alias. Files in the Target Path are supposed as scripts, such as CGIs, implicitly. This is useful when executing those CGI files that do have end with the extension .cgi.
ScriptAliasMatch	Similar to ScriptAlias except users can use regular expressions for the Source URL as well as the back reference such as $1, $2.... for the Target URL.

● Source URL

Enter the source URL to be accessed.

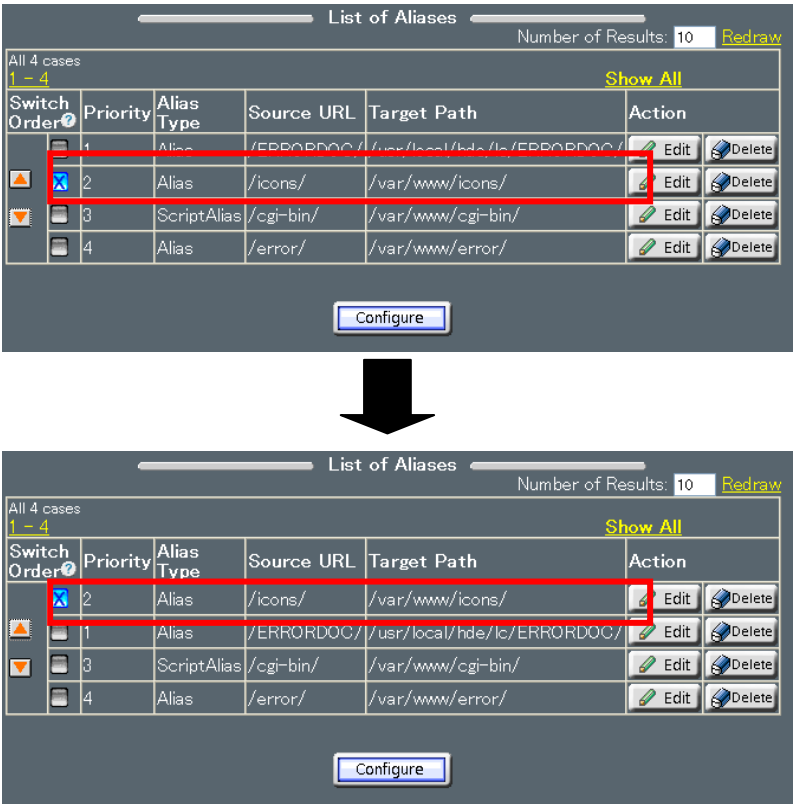
- Target Path

  Enter or select from "Select Directory" the target path of the actual path of the file system when the address is accessed.

■ Changing Alias Priority

Change the priority of the added alias.

Select the row of the alias you wish to change the priority (multiple selections possible) and click the UP and DOWN arrows to move the row and change its priority.



After changing the priority of the alias, click the "Configure" button on the button to save your settings.

The alias configurations will be assessed in the ascending-order of the alias priority values. Please note that specifying a subset of a high priority alias to a lower priority will not work.

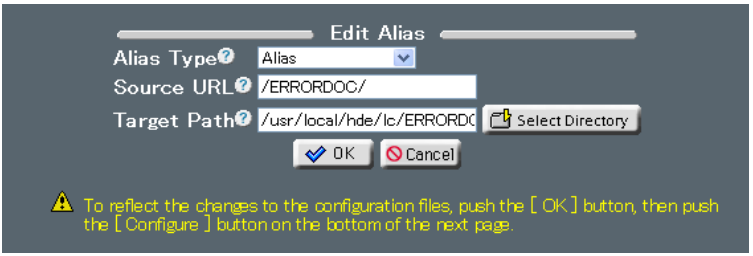
Ex)

Priority	AliasType	Source URL	Target Path
1	Alias	/abc	/var/www/abc
2	ScriptAlias	/abc/def	/var/www/def

In this case, even if the user tries to access /abc/def, the rule of /abc (higher priority) will apply and the user will be lead access to /var/www/abc/def instead of /var/www/def.

■ Editing Alias

Edit the alias values of existing alias. Click on the "Edit" button of the alias you wish to edit.



Change the Alias Type, Source URL, and Target Path and click the "OK" button.

After completing all of the setting changes, click on the "Configure" button to save your configurations.

6. MIME Type Settings

Configure the MIME type settings for the Web server to recognize incoming data formats.

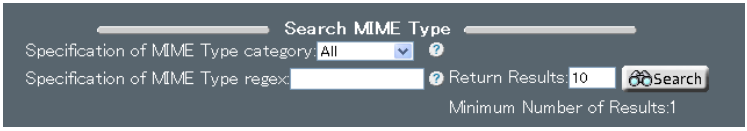
MIME type defines the characteristics of the files on the Web server which are accessed by the clients and is specified by a list of strings in the format of "Type Name/Sub-Type Name".

By configuring the settings of MIME Type, the Web server will be able to provide accurate information to the clients.

■ Search MIME Type

Search the registered MIME types.

Select the search parameters from the "Specification of MIME Type category" menu.



Enter the search keyword into the "Specification of MIME Type regex" field.

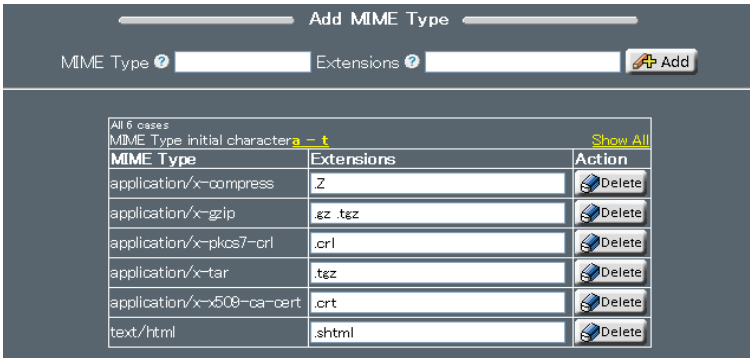
To change the number of search results, change the value in "Return Results".

Click the "Search" button to begin your search.

To search the MIME types by their initials, click on the range of initial defined by "MIME Type initial character" on the top of the search list. To show all registered MIME types at once, click on "Show All".

■ Add MIME Type

Add a new MIME type to the list of registered MIME types.



- MIME Type

  Enter the MIME type you wish to add in the "MIME Type" field (Ex. video/mpeg).

- Extensions

  In the "Extensions" field, enter the file extension of the new MIME type used for identifying the MIME type (Ex. mpeg).

  Click the "Add" button to add the new MIME type.

  You may also change the file extensions of the MIME types that are already registered to the system by changing the "Extensions" field on the list of MIME types.

  Click the "Delete" button to delete a MIME type. Click the "Undo" button to undo your deletion.

  Click the "Configure" button to complete your settings.

7. ModSecurity Settings

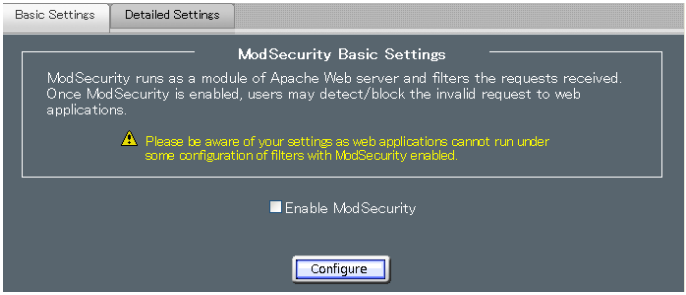
Configure the ModSecurity Settings.

ModSecurity functions as a module to the Web server Apache which filters the requests sent to the Web server. By using ModSecurity, users are able to seek out and block harmful access attempts to the Web applications.

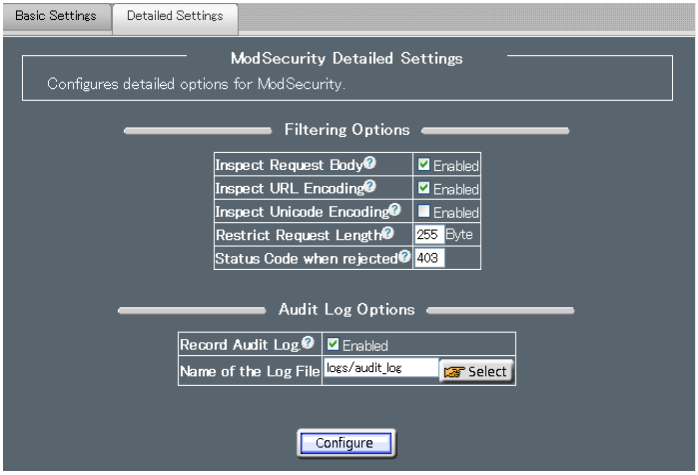
■ Basic Settings

Users may enable ModSecurity settings by checking the "Enable ModSecurity" box and clicking the "Configure" button.

> ⚠ Please note that when ModSecurity is enabled, some of the Web application may not function properly depending on your filter settings.



■ Detailed Settings



Perform the detailed configurations of ModSecurity. Users are not required to make any changes to this setting under normal conditions.

● Inspect Request Body

Enable this to inspect request body. Requests returned by the GET method contain no body content. The requests returned by the POST method contain the data in the body.

● Inspect URL Encoding

Check whether the URL encoding is valid.

● Inspect Unicode Encoding

Check whether the Unicode encoding is valid.

● Restrict Request Length

Specify the maximum request length (bytes) to be allowed. The data using multipart/form-data is not restricted.

- Status Code when Rejected

  Specify the status code replied when matching the rules and denying the request.

- Record Audit Log

  Enable this to log the request which matched the rules and was denied.

- Name of the Log File

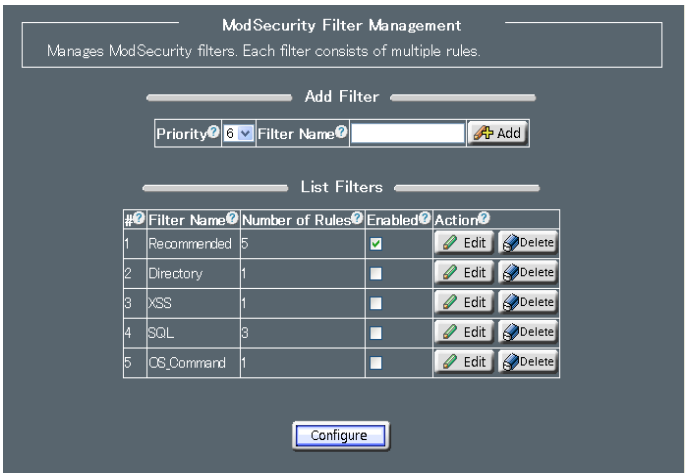
  Specify the file name of the record audit log.

8. ModSecurity Filter Management

Configure the filtering rules of the ModSecurity modules. This setting will manage multiple rules and apply them to the Web server as a filter.

■ Add Filter

Add a new filter



Specify the "Priority" and "Filter Name" of the new filter and click the "Add" button to add the filter to the list. Please note that the filtering rules will not be applied just by adding a new filter. Please click on the "Edit" button of the newly added filter to configure the filtering rules.

● Priority

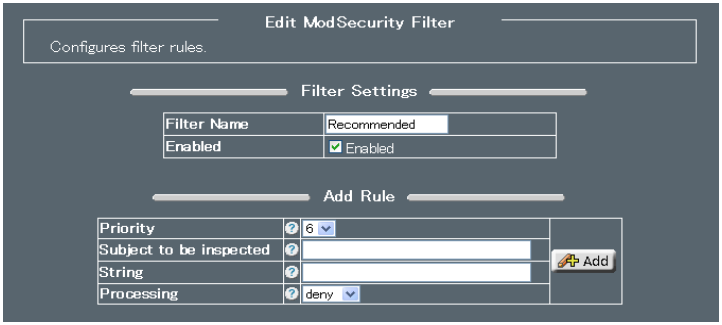
The newly added filter will be inserted into the specified priority position and the priority of any existing lower priority filters will be moved down by 1. The filters will be applied in the ascending-order of their priority values.

● Filter Name

Filter Name. Use letters, numbers, [-] and [_] in 20 chars.

Please note that any filters in the list without their "Enabled" box checked will not be applied. Please enable the filters by checking the "Enabled" box and then click on the "Configure" button.

■ Add Rule



Specify the "Priority", "Subject to be inspected", "String", "Processing" fields and click on the "Add" button.

- Priority

  Set the priority of the rule to be added. The filter will be inserted into the specified position. Increments the priority by one if the specified position is already occupied.

- Subject to be inspected

  Specify the inspection target. If multiple entry exists, separate each entry with [|]. If omitted, the inspection targets will be set as all of the incoming requests. For detailed explanation on how to enter this field, please refer to the "Request Filtering" and "Advanced Filtering" sections of the ModSecurity manual.

- String

  Search word. Users may enter using regular expressions.

- Processing

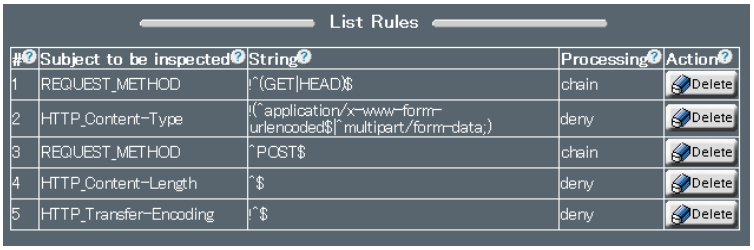
Configure the actions to be executed when the target matches with the search word.

deny	Denies the request and return the status code defined in "ModSecurity Settings" - "Detailed Settings" - "Status Code when rejected".
pass	Do nothing. Logs the request if "ModSecurity Settings" - "Detailed Settings" - "Record Audit Log" is enabled.
allow	Accepts the request and disable any rules that apply afterwards.
chain	The next rule will be applied only when matching the current rule.

■ Editing and Deleting the Settings

To delete filters or filtering rules, click the "Delete" button and then click on the "Configure" or "OK" button.

Similarly, to edit filters or filtering rules, click the "Edit" button to bring up the edit screen similar to that of adding a new filter or rule. Change the settings of the fields as necessary.



■ Example of Filter Setting

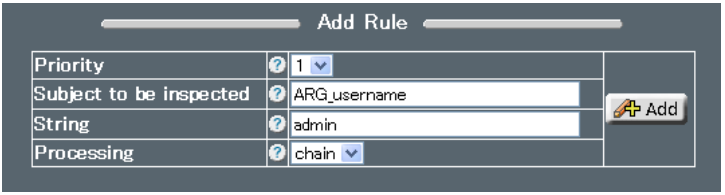
As an example, we will set a filter to a Web application administrator account which only allows login from specified IP address and blocks access from any other IP addresses.

First, add a new filter to the list of filters. Please proceed to the "ModSecurity Filter Management" screen. Specify the filter name as "admin" and filter priority as "6". After entering the filter name and priority, click on the "Add" button to continue.

Your newly added filter will now be displayed in the list of filters. Next, you will register the filtering rules of your filter. Please click on the "Edit" button to continue.

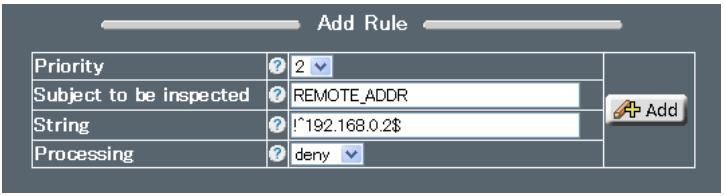
Specify "Priority" as "1", "Subject to be inspected" as "ARG_username", "String" as "admin", and "Processing" as “chain” then click the "Add" button to continue.

"ARG_username" refers to the variable which is defined as "username". The rule configured here will be applied when the "username" variable includes the string "admin".



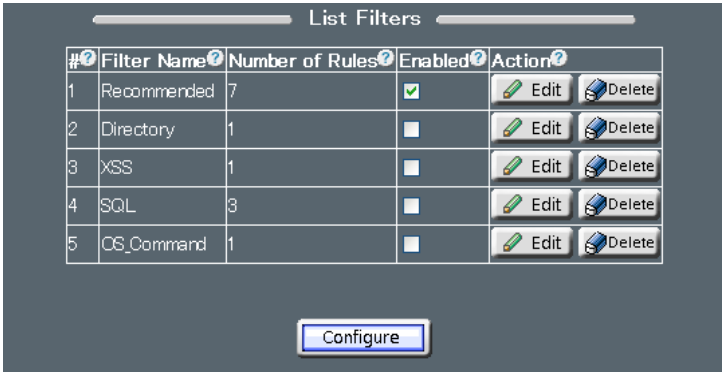
For the next rule, specify "Priority" as "2", "Subject to be inspected" as "REMOTE_ADDR", "String" as "!^192.168.0.2$", "Processing" as "deny" and click the "Add" button.

"REMOTE_ADDR" refers to the IP address of the client trying to access the Web server. The rule added here specifies that if the client IP address does not match with "192.168.0.2", the filter will deny access of the client.



After registering the rules, click on the "OK" button to continue.

Make sure that the filter is checked as "Enabled" in the "List of Filters" and click the "Configure" button to apply your configurations.

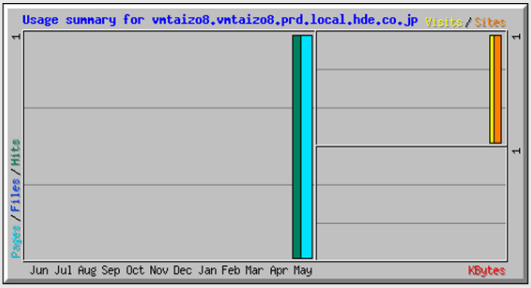

List Filters
Filter Name Number of Rules Enabled Action
1 Recommended 7 Edit Delete
2 Directory 1 Edit Delete
3 XSS 1 Edit Delete
4 SQL 3 Edit Delete
5 OS_Command 1 Edit Delete
Configure

9. Access Statistics Report

Analyze the Web server logs and display the analysis results.

Users are allowed to use the following functions: monthly statistics, daily statistics, hourly statistics, hit-count ranking (URLs, entries, Exits, sites,), referrers, search strings, user agent, and country-wise statistics.

The statistics of the past 12 months will first be displayed when the "Access Static Report" menu is clicked.



月の統計

月	一日あたりの平均				月合計					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
May 2011	1	0	1	1	1	0	1	1	0	1
総合計						0	1	1	0	1

The definitions of each indexes displayed are as follows:

Hits	Total number of accesses made to the server (including errors).
Files	Total number of normal accesses within the number of “Hits”.
Pages	Total number of HTML page accesses within the number of “Hits”
Visits	Total number of visitors. (Does not include access from the same IP address within a 30 minutes time frame).
Sites	Total number of visitors (Does not include access from the same IP address).
KBytes	Total amount of data transferred.

You may display statistics of months other than the currently month by clicking the link of each months.

HDE Controller PRO / LG User Manual

April 30, 2011 1st Ed. 10.0-001

HDE, Inc.

16-28, Nanpeidaicho, Shibuya, TOKYO, 150-0036 JAPAN