

## **Doteasy KB**

### **How do I set Domain rules?**

Doteasy Email Protection System can make decisions based just on the domain part of the email address. The domain part is everything after the "@" sign. For example, the domain part of staff@doteasy.com is Doteasy.com.

To see the domain rules list, click on Rules and then Domains.

The columns in the table are:

- a) Domain – the domain name of a sender
- b) Who – the user who last modified the sender's disposition
- c) Action – the action taken by Doteasy Email Protection System when a message from the domain arrives. Possible actions are:

No Change – keep the current action  
Always Allow – always allow mail from this domain without scanning for spam. (note: dangerous attachments are still scanned and stripped)  
Always Hold for Approval – mail from this domain is always held for approval, even if spam-scanning does not flag it as spam.  
Hold if Looks Like Spam – this is the default action; mail from this domain will be held if it scores high enough on the spam scale  
Always Reject – messages from this domain are always rejected with a permanent failure code.  
Delete from Table – the domain is deleted from the table. Also, Doteasy Email Protection treats the domain as if the setting Hold if Looks Like Spam had been used.

- d) Expiry – You can specify the effective period of this rule.

- e) Comment – allows you to enter a comment if you like. This can help you remember why you whitelisted or blacklisted a domain.

To set new actions, adjust the Action entries appropriately and click on the Submit Changes button.

If you want to set an action for a domain that is not in the domain list, enter the domain name in the text box and click on the Add Rule button. You will then be asked to set the action for that domain name.

Click on Always Allow , Always Hold for Approval , Hold if Looks Like Spam , Always Reject or All to restrict the domain page to domains who are always allowed, always held, held if the message looks like spam, always rejected, or all domains, respectively.

Note : Suppose you receive email from user@mail.sub.domain.net, the Doteasy Email Protection System performs the following domain lookups:

mail.sub.domain.net sub.domain.net domain.net net

Thus, if you disallow email from domain.net, your Doteasy Email Protection System also automatically sub.domain.net and mail.sub.domain.net. However, you can explicitly allow sub.domain.net by adding another entry, because a domain with more components is more specific than, and takes preference over,

one with fewer components.

<https://kb.doteasy.com/questions/363/>