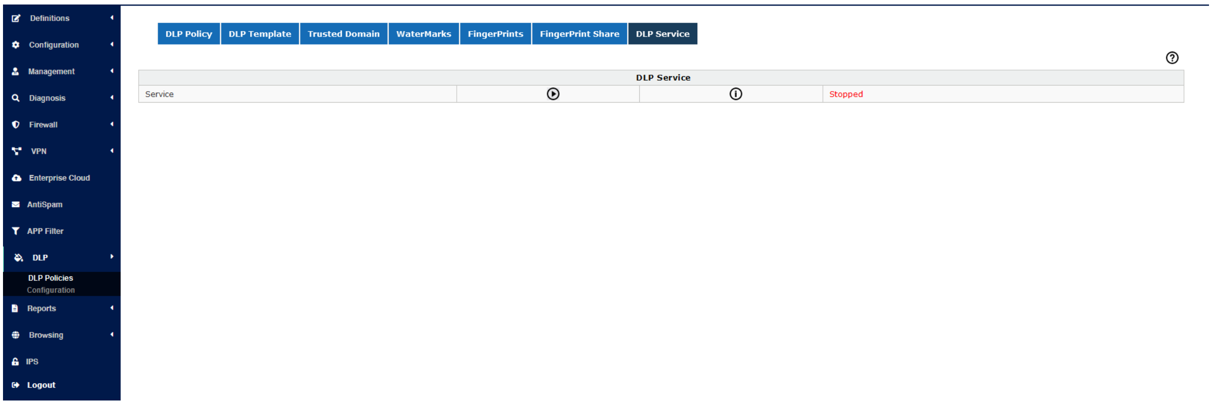
GAJSHIELD
Data Security Firewall

How to configure DLP policy to block personal Facebook login

How to configure DLP policy to block personal Facebook login

NOTE: Before you begin DLP configuration it is important to check if the DLP service is running.

You can do so by going to DLP-> DLP Policies -> DLP Service



DLP Service			
Service	▶	ⓘ	Stopped

Once you check that the DLP Service is running, you can begin your configuration.

To create a new DLP policy to block personal Facebook login, go to DLP -> DLP Policies -> DLP Template.

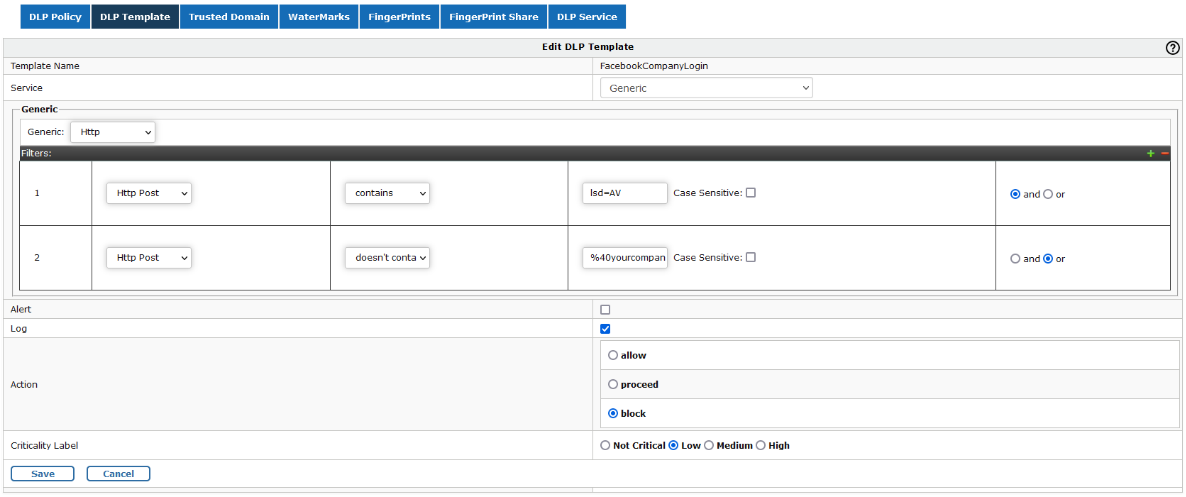
To add a new DLP policy template, click on ⊕ icon.

Click on Add button and add a new DLP template

To add from Available DLP templates to selected DLP Templates, select the template and click on ▸ button.

To remove Selected DLP Templates, press ◂ button.

You can also Select the already existing template and edit it. For instance, select the template FacebookCompanyLoginblock and specify the following information.



Edit DLP Template

Template Name	FacebookCompanyLogin
Service	Generic

Generic

Generic: Http

Filters:

1	Http Post	contains	lsd=AV Case Sensitive: □	● and ○ or
2	Http Post	doesn't conta	%40yourcompan Case Sensitive: □	○ and ● or

Alert	□
Log	☑
Action	○ allow ○ proceed ● block
Criticality Label	○ Not Critical ● Low ○ Medium ○ High

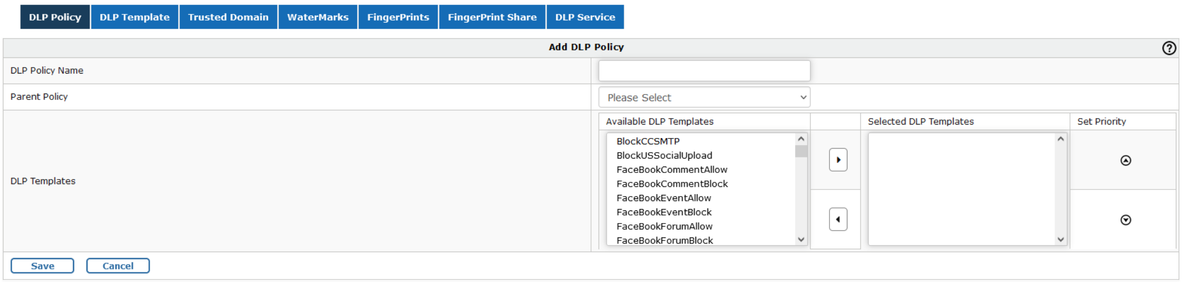
Save Cancel

In the filters, you can specify the details of your company in the place of "yourcompany.com" This will allow only your company login to be accessed while the rest of the personal logins attempted will be blocked.

Now add these templates into your DLP policy by going to DLP -> DLP policies -> DLP policy.

You can set the priority of the selected DLP Templates by moving them up or down using these buttons. Click on ⏶ button to increase the priority level and click on ⏷ button to decrease the level of priority. The topmost template in the list has the highest priority whereas the template at the last has least priority.

You can select the templates you wish to add to the policy from the available DLP Templates list to enable the DLP, if there are no templates set in DLP policy, the new DLP policy won't be allowed to be created. You need to add at least one DLP template for the policy to be created.



Add DLP Policy

DLP Policy Name	
Parent Policy	Please Select
DLP Templates	Available DLP Templates: BlockCCSMTP BlockUSSocialUpload FaceBookCommentAllow FaceBookCommentBlock FaceBookEventAllow FaceBookEventBlock FaceBookForumAllow FaceBookForumBlock Selected DLP Templates Set Priority

Save Cancel

NOTE: After adding the new DLP policy, you need to make sure that policy is added in the firewall rule by going into Firewall -> Policies -> Rules. You need to add those rules there in order to be able to successfully apply the DLP policies. Make sure the Deep Inspect option is enabled while configuring the firewall rules to get DLP visibility for HTTPS (SSL) secure traffic.

Thus, we have added the DLP policy for the complete network as seen above. You can also add it to an individual group or selected groups as per your network requirement.