# How do you use regular expressions (regex) with grep to search logs?

**Document ID: 118422**

Contributed by Cisco TAC Engineers.
Oct 13, 2014

## Contents



## Question

How do you use regular expressions (regex) with grep to search logs?

## Environment

Cisco Web Security Appliance
Cisco Email Security Appliance
Cisco Security Management Appliance

## Solution

Regular expressions (regex) can be a powerful tool when used with the "grep" command to search through logs available on the appliance, such as Access Logs, Proxy Logs, and others. We can search the logs based on the website, or any part of the URL, or user names, to name a few, when using the CLI command "grep".

Below are some common scenarios where you can use regex with grep to assist with troubleshooting.

### Scenario 1: Finding a Particular Website in the Access Logs

The most common scenario is attempting to find requests being made to a website in the access logs of the Cisco Web Security Appliance (WSA).

For Example:
Connect to the appliance via SSH. Once you have the prompt, we can type the "grep" command to list the available logs.

| ***CLI***> grep |
| --- |
| Enter the number of the log you wish to "grep". |

| |
|---|
| []> 1 (Choose the # for access logs here) |
| Enter the regular expression to "grep".<br>[]> ***website\.com*** |

## Scenario 2: Attempting to Find a Particular File Extension or Top−Level Domain

We can use the "grep" command to find a particular file extension (.doc, .pptx) in a URL or a top−level domain (.com, .org).

For Example:
To find all URLs that end with .crl we could use the following regex: ***\.crl$***

To find all URLs that contain the file extension .pptx, we could use the following regex: ***\.pptx***

## Scenario 3: Attempting to Find a Particular Block For a Website

When searching for a particular website, we might also be searching for a particular HTTP response.

For Example:
If we wanted to search for all TCP_DENIED/403 messages for domain.com, we could use the following regex: ***tcp_denied/403.*domain\.com***

## Scenario 4: Finding a Machine Name in the Access Logs

When using NTLMSSP authentication scheme, we may come across an instance where a User Agent (Microsoft NCSI is the most common) will incorrectly send machine credentials instead of user credentials when authenticating. To track down the URL/User Agent that causes this, we can use regex with "grep" to isolate the request made when the authentication occurred.

If we do not have the machine name that was used, we can use "grep" and find all machine names that were used as user names when authenticating using the following regex: ***\$@***

Once we have the line where this occurs, we can "grep" for the specific machine name that was used by using the following regex: ***machinename\$***

The first entry that comes up should be the request that was made when the user authenticated with the machine name instead of the user name.

## Scenario 5: Finding a Specific Time Period in the Access Logs

By default, access log subscriptions will not include the field that shows the human readable date/time. If we want to check the access logs for a particular time period, we can follow the steps below:

Look up the UNIX timestamp from a site such as http://www.onlineconversion.com/unix_time.htm. Once you have the timestamp, you can search for a specific time within the Access Logs.

For Example:
A Unix timestamp of 1325419200 is equivalent to 01/01/2012 12:00:00.

We can use the following regex entry to search the access logs around the time of 12:00 on January 1st, 2012:
13254192

## Scenario 6: Searching for Critical or Warning Messages

We can search for critical or warning messages in any available logs, such as proxy logs or system logs, using regular expressions.

For example:
To search for warning messages in the proxy logs, we can enter the following regex:

1. ***CLI***> grep
2. Enter the number of the log you wish to "grep".
   []> 17 (Choose the # for proxy logs here)
3. Enter the regular expression to "grep".
   []> ***warning***

Other useful links:

Regular Expressions − User Guide

Updated: Oct 13, 2014 Document ID: 118422