OpenVMS System Parameters
Controlling Login & Break-in Detection

The following SYSGEN parameters control login behavior and can be used to control break-in detection and evasive actions under OpenVMS.

Parameter	Default Value	Description[1]
LGI_BRK_DISUSER	0 (True/False)	Turns on the DISUSER flag in the UAF record when an attempted break-in is detected, thus permanently locking out that account. The parameter is off (0) by default. You should set the parameter (1) only under extreme security watch conditions, because it results in severely restricted user service.
LGI_BRK_LIM	5 (Failures)	Specifies the number of failures that can occur at login time before the system takes action against a possible break-in. The count of failures applies independently to login attempts by each user name, terminal, and node. Whenever login attempts from any of these sources reach the break-in limit specified by LGI_BRK_LIM, the system assumes it is under attack and initiates evasive action as specified by the LGI_HID_TIM parameter.
LGI_BRK_TERM	1 (True/False)	Causes the terminal name to be part of the association string for the terminal mode of break-in detection. When set to off (0), the processing considers the local or remote source of the attempt, allowing break-in detection to correlate failed access attempts across multiple terminal devices. When set to on (1), LGI_BRK_TERM assumes that only local hard-wired or dedicated terminals are in use and causes break-in detection processing to include the specific local terminal name when examining and correlating break-in attempts.
LGI_BRK_TMO	300 (Seconds)	Specifies the length of the failure monitoring period. ***This time increment is added to the suspect's expiration time each time a login failure occurs.*** Once the expiration period passes, prior failures are discarded, and the suspect is given a clean slate.

Parameter	Default Value	Description[1]
LGI_CALLOUTS	0 (Count)	Specifies the number of installation security policy callout modules to be invoked at each login. LGI_CALLOUTS must be set to 0 unless callout modules are present.
LGI_HID_TIM	300 (Seconds)	Specifies the number of seconds that evasive action persists following the detection of a possible break-in attempt. The system refuses to allow any logins during this period, even if a valid user name and password are specified.
LGI_PWD_TMO	30 (Seconds)	Specifies, in seconds, the period of time a user has to enter the correct system password (if used). LGI_PWD_TMO also establishes the timeout period for users to enter their personal account passwords at login time. Also, when using the SET PASSWORD command, LGI_PWD_TMO specifies the period of time the system waits for a user to type in a new password, an old password, and the password verification.
LGI_RETRY_LIM	3 (Tries)	Specifies the number of retry attempts allowed users attempting to log in. If this parameter is greater than 0, and a legitimate user fails to log in correctly because of typing errors, the user does not automatically lose the carrier. Instead (provided that LGI_RETRY_TMO has not elapsed), by pressing the Return key, the user is prompted to enter the user name and password again. Once the specified number of attempts has been made without success, the user loses the carrier. As long as neither LGI_BRK_LIM nor LGI_ BRK_TMO has elapsed, the user can dial in again and reattempt login.
LGI_RETRY_TMO	20 (Seconds)	Specifies the number of seconds allowed between login retry attempts after each login failure. (Users can initiate login retries by pressing the Return key.) This parameter is intended to be used with the LGI_RETRY_LIM parameter; it allows dialup users a reasonable amount of time and number of opportunities to attempt logins before they lose the carrier.

You can also obtain a copy of this document at this link:

http://www.migrationspecialties.com/pdf/SYSGEN Login Parameters.pdf

---

[1] Parameter descriptions have been pulled almost verbatim from the *HP OpenVMS System Management Utilities Reference Manual: M – Z, Appendix C: System Parameters*.