

Migration Specialties International, Inc.

217 West 2nd Street, Florence, CO 81226-1403

+1 719-371-1711, Fax: +1 888-854-3417

E-mail: Info@MigrationSpecialties.com

www.MigrationSpecialties.com



Bruce Claremont, July, 2006

Adventures in Consulting: OpenVMS System Login Parameters Sheet for Site Security Manual

I recently inadvertently became involved in a site security audit. I happen to be at a client site providing unrelated OpenVMS services when the audit took place. The end result is the login parameter sheet at the end of this story. Here is what transpired.

I was chugging away at some mundane, but critically important tasks when the CIO and attendant staffers appeared at my side with an auditor in tow. He was a handsome fellow, still upright and fit. Not yet bowed by the frustrations and bitterness inherent in his profession.

"Bruce," said the CIO, "Tim here has some questions concerning controlling login access to the VMS systems."

Well, far be it from me to miss an opportunity to talk up the security features of OpenVMS. I launched into a description of the UAF file and AUTHORIZE utility, touched on UIC and ACL security features, and topped things off with standard break-in evasion procedures.

Much to my surprise, while the CIO and attendants had nodded off, Tim's eyes hadn't glazed over and he still seemed pretty interested. Consulting a set of closely guarded notes, he said:

"That's all well and good, but what I am really interested in is how you control logins at the system level."

Thinking about this for a microsecond, I snapped the OpenVMS documentation CD into my laptop, open up the *OpenVMS System Management Utilities Reference Manual: M – Z*, and located the LGI SYSGEN parameters.

"Is this what you mean," I asked?

"Wow," said Tim. "That's all part of the standard operating system?"

"That's right," I responded.

Whereupon Tim flashed a smile so bright it woke the CIO. A brief ripple of panic crossed her face before she recognized the smile as one of pleasure, not incrimination.

"If you'll document those parameters for our *IT Site Security Manual*, I'll be satisfied that OpenVMS is a secure operations platform," said Tim.

"No problem, consider it done," said the CIO as the group departed. She flashed me a well done wink as she went out the door.

Here's the document I put together for their Site Security Manual. It's not extensive and it's pretty much verbatim from the OpenVMS manual. Its purpose is to provide an overview of the system parameters available under OpenVMS to protect against illegal login access to the system, nothing more. Perhaps some of you dear readers will find it useful.

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. <i>This time increment is added to the suspect's expiration time each time a login failure occurs.</i> Once the expiration period passes, prior failures are discarded, and the suspect is given a clean slate.
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.

Parameter	Default Value	Description ¹
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*.