eG

Enabling Service Excellence

Hardening the Security of eG Enterprise

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations, Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows 2008, Windows 2012, Windows 2016, Windows 7, Windows 8, and Windows 10 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

How to Harden the Security of eG Enterprise?

If you are going to deploy the eG manager and/or the eG agent on the cloud, you need to ensure that it is secure and guard it against different forms of cyber attacks. Here are many checks and safeguards that you should put in place for this.

Category	Security check	Remarks
Installation checks	Have you configured your eG manager to use the latest supported version of the Java Development Kit (JDK)?	Using the latest supported JDK (JDK 12) will ensure highest level of security to the eG manager.
	Are the eG manager and database running on the same system? If so, have you configured the firewall to block all external connections to the database server?	eG agents and users of the eG Enterprise system do not directly communicate with the eG database. Only the eG manager communicates with the database. Hence, allowing only internal connections from the eG manager and preventing connections from external sources to the eG database, will shield the eG Enterprise system from unexpected cyber attacks.
	Have you configured the firewall of the operating system (eg., Windows) hosting the eG manager to allow access to only the eG manager's port?	All communications to the eG manager happen over one TCP port. Configure firewall rules to limit accesses to the eG manager system to this pre-configured TCP port.
	Have the latest service packs and patches been deployed on the server hosting the eG manager?	Ensure that the latest service packs and hot fixes are applied for the operating system on which the eG manager is hosted.
SSL checks	Has eG manager been SSL-enabled?	Ensure that the eG manager is SSL-enabled, so all communications between users/agents and the eG manager happen over secure HTTP connections. Refer to the *eG Installation Guide* to know how to SSL-enable the eG manager.
	Have you included a strong Cipher Suite definition in your eG manager?	A cipher is any method of encrypting text (concealing its readability and meaning). Cipher suite is a concept used in Transport Layer Security (TLS) / Secure Sockets Layer (SSL) network protocol. It is a named combination of authentication, encryption, message authentication code (MAC) and key exchange algorithms used to negotiate the security settings. When a TLS connection is established, a handshaking, known as the TLS Handshake Protocol, occurs. Within this

		handshake, the client sends a list of the cipher suites that it supports, in order of preference. Then the server replies with the cipher suite that it has selected from the client's list. Recent versions of Firefox and Chrome reject HTTPS requests to the eG manager, if they do not contain the strong Cipher Suite definitions they expect. In other words, if users try to connect to an SSL-enabled eG management console using the latest version of Firefox or Chrome, then the handshake between the browser client and the eG manager server will fail, if the eG manager is not configured with the strong Cipher Suite definitions these browsers support. To avoid this, you should configure the eG manager to include a strong Cipher Suite definition. Refer to the *eG Installation Guide* to know how to achieve this.
	Has TLS 1.2 been enabled for the eG manager?	To ensure that the communication between a browser client (Chrome, Firefox, or IE) and an SSL-enabled eG manager is fully secure and encrypted, it is recommended that you disable SSL and enable TLS 1.2 on your browser. This is because, after the POODLE vulnerabilities that were discovered recently, even the latest version of SSL – SSL v3.0 – has been declared as insecure for web sites using it. Refer to the *eG Installation Guide* to know how to enable TLS for the eG manager.
	Is the eG agent monitoring SSL-enabled applications? If so, has the SSL certificate of the target application been imported into the JRE of the eG agent?	The steps for importing the SSL certificate of an application into the JRE of an eG agent are the same as the steps for importing the SSL certificate of the eG manager into the JRE of an eG agent. These steps have been detailed in the *eG Installation Guide*.
Access checks	Have you changed the password of the admin and supermonitor users?	Admin and supermonitor are pre-defined accounts that are enabled on the eG manager. Ensure that you change the password for these accounts once you set up the eG manager. This will prevent unauthorized access. Refer to the *Administering eG Enterprise* document to know how to change the password for admin and supermonitor users.
	Has account locking been enabled?	The Account Locking feature enables the eG manager to protect the eG Enterprise system from malicious users. If this lockout feature is enabled for the eG manager, then, if a user's attempt to login to the eG management console fails a configured number of times, the eG Enterprise system will automatically 'lock' that user account. In this case, the user will not be able to login until: • The expiry of a configured period of time, or; • The administrator manually unlocks the account using the eG administrative interface

		Refer to the *Administering eG Enterprise* document to know how to enable account locking.
	Has audit logging been enabled?	An audit log can be best described as a simple log of changes, typically used for tracking temporal information. The eG manager can be configured to create and maintain audit logs in the eG database, so that all key configuration changes to the eG Enterprise system are tracked. The eG audit logs reveal critical change details such as what has changed, who did the change, and when the change occurred, so that administrators are able to quickly and accurately identify unauthorized accesses/modifications to the eG Enterprise system. Refer to the *Administering eG Enterprise* document to know how to enable audit logging.
Vulnerability checks	Is the TCP time stamp response vulnerability checked on the eG manager system?	Vulnerabilities in TCP Timestamps retrieval is a Low risk vulnerability, but is one of the most frequently found vulnerabilities on networks around the world. The eG manager host typically responds to each TCP connection request to it with a TCP timestamp response. Malicious users can use this timestamp response to approximate the manager host's uptime, potentially aiding in further attacks. Moreover, some operating systems can even be fingerprinted based on the behaviour of their TCP timestamps. TCP time stamp response vulnerabilities are by default enabled in the eG manager. This ensures that TCP timestamp responses from the eG manager system are automatically disabled.
	Is click jacking checked?	Click jacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. Click jacking checks are by default enabled in the eG manager. This ensures that if a user clicks on an iFrame in the eG user interface that embeds one/more URLs to a different site or application, such links are automatically disabled. Only those URLs in an iFrame that link users to web pages within the eG manager application will be allowed.
	Is the eG manager hardened against cross site scripting attacks?	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application, such as the eG manager. The eG manager is by default hardened against cross-site scripting attacks.

	Are CSRF security checks turned on?	Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. CSRF security filters are by default enabled on the eG manager.
	Is SQL injection checked?	SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQLstatements (also commonly referred to as a malicious payload) that control a web application's database server (also commonly referred to as a Relational Database Management System – RDBMS). The eG manager is by default hardened against SQL injection attacks.
	Have all cookies sent over HTTP secured?	To achieve this, do the following: 1. Login to the eG manager host. 2. Edit the context.xml file in the <EG_MANAGER_INSTALL_DIR>\manager\tomcat\conf directory. 3. Add the following attribute in the file with the context tag: *<Context useHttpOnly="true" privileged="true">* 4. Finally, save the file.