Genasys Emergency Management (GEM) Enterprise Deployment Security

Enterprise Deployment Security

GEM Enterprise is deployed as a server-based solution that incorporates the operating system and one or more application services in a single wizard-based installation. Typically, the software appliance is installed as a guest host in a VM environment, but also supports installation on standalone server platforms.

Deployments are never shared between different customers. This extends to third-party services (i.e. SMS, callout, and push notification services), where each customer maintains their own third-party accounts separate from Genasys Communications Canada (GCC) and other customers

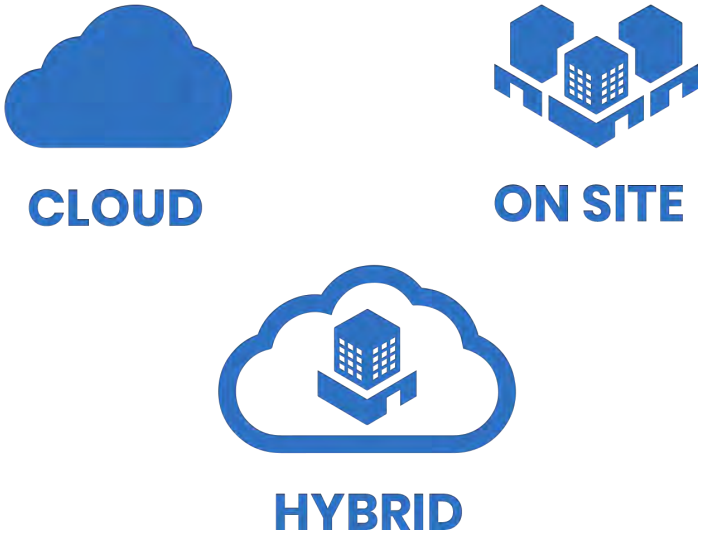
Private Network - Cloud

When deployed in the cloud, GEM servers are hosted either within each customer's own private cloud infrastructure or within AWS/Azure IaaS private cloud facilities. The AWS and Azure compliance guarantees are well documented (see https://aws.amazon.com/compliance and https://azure.microsoft.com/en-ca/overview/trusted-cloud/compliance/).

Private cloud deployments can be managed by either the customer, subject to their security practices, or by GCC, in which GCC applies best practices for hosted solutions and can adjust when requested by the customer's IT team

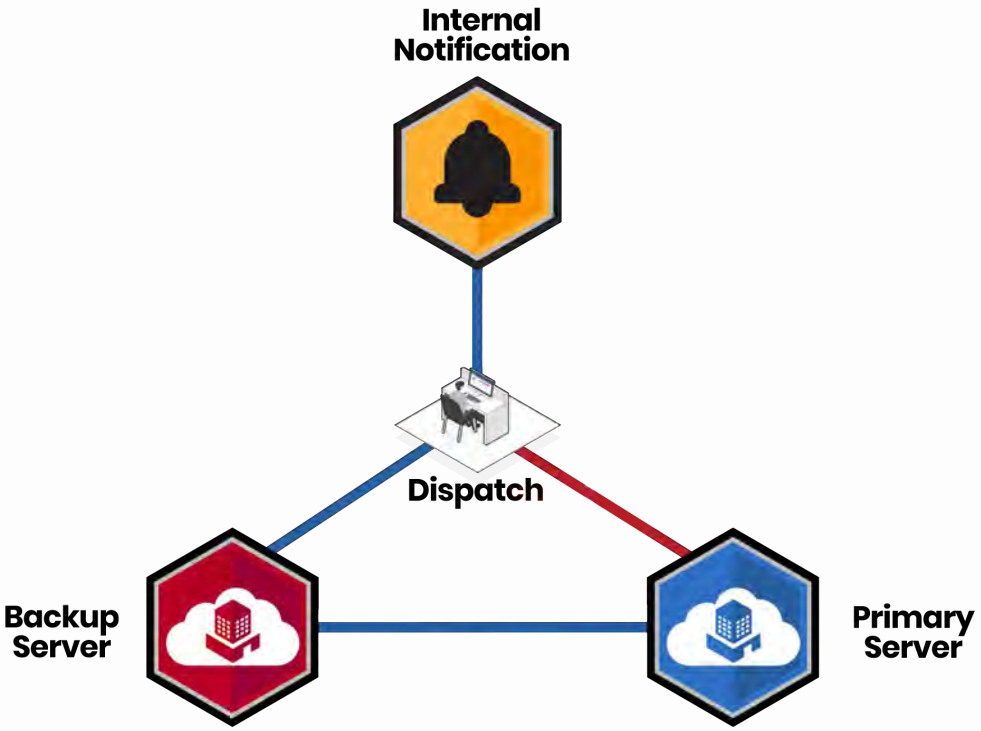
Private Network - On-Premise

When deployed on the customer premises, access to GEM servers are subject to each customer's security practices.



Genasys™

GEM
Enterprise Availability



Availability

GEM servers are normally deployed in a fully redundant mode, with designated Primary and Backup (active/active) servers. The servers are robust, self-managing Linux-based machines that are extremely resistant to operating system and application failure and require only minimal monitoring or intervention. In a monitored private-cloud environment with geographical separation, availability is expected to be 99.99% between the two servers. In an on-premises deployment the customer is responsible for server location, power, the VM host environment and networking. In most situations 99.99% uptime is observed.

Change Control

GEM Enterprise feature updates generally occur two to three times a year, with interim security upgrades provided when necessary. Customers are informed of upgrade availability through their dedicated Support contact, who provides Release Notes describing the changes. Customers control when an upgrade is performed. In redundant deployments, the Backup server can be upgraded separately from the Primary for acceptance and training purposes.

Genasys™

GEM Enterprise Access Control

Access Control

Access to the web-based operations and administration console on a GEM server may be configured in any of the following ways:

- Using local credentials created and stored in the server's database. Such credentials are protected by a one-way hashing algorithm compliant with FIPS 140-2.
- Using domain-based credentials, where the domain accounts are configured on the GEM server or identified as being members of a domain distribution group. This requires integration with an LDAP-based domain server (e.g. Active Directory). Credentials are verified against the domain server using FIPS 140-2-compliant encryption in transit. To account for network connectivity issues, credentials are also stored
- Using Single Sign-On (SSO). GEM Enterprise supports the SAML 2.0 authentication protocol. The SSO integration enables federation between the GEM Enterprise Console and Identity Providers (IDPs) such as Okta, PingIdentity, Shibboleth and ADFS. This capability supports usage of the redirect, post, and artifact bindings for SSO authentication, with support for accepting a standard-based assertion sent from the IDP. Multiple IDPs are supported. Role-based access is supported, including using standards-based schemas such as eduPerson. All credential-associated data is exchanged using FIPS 140-2-compliant encryption in transit

Intrusion Detection

GEM Enterprise allows configuration of a limit on invalid authentication attempts on individual browser sessions and supports limiting the login attempts to specific known IP addresses or IP address ranges. It can also be configured to disallow multiple simultaneous logins to the same account. Additionally, GEM Enterprise protects against denial of service attacks, incorporating sophisticated features to detect and "tarpit" or deny repeated attacks across all open ports. Furthermore, when GEM Enterprise is delivered within the AWS IaaS environment, additional protection can be included using their services.

Role-Based Access

Privileges are assigned to operators and administrators according to organizational requirements in terms of managing configurations, issuing and monitoring alerts, and accessing database information.

Replay Resistance

GEM server connections are "replay resistant". Session identifiers are always invalidated upon user logout or other session termination, including non-activity timeouts. Unique session identifiers are generated for each session. The servers recognize only session identifiers that are system-generated, and only allow the use of Internet and/or customer certificate authorities for verification of the establishment of protected sessions.

Genasys™

GEM Data Protection

Data Protection

GEM servers use FIPS 140-2-compliant encryption or hashing for protected data at rest, and leverage FIPS 140-2 secure SSL for protecting data in transit. Current encryption standards used are: AES256/CBC encryption, RSA2048 for key establishment, SHA512 hashing, and SHA256 for HMAC authentication. Current SSL standards used are: TLS 1.2 encryption (TLS 1.3 coming soon). GEM servers incorporate a firewall, which is used to lock down access to specific origination IP ranges and ports based on customer access and integration requirements.

End-user (recipient) information may be stored on the GEM server database or may be held externally in a controlled database or directory. Depending on the deployment requirements, recipient information may not be required if only anonymous alerting is required. On-server data can be purged from the system immediately after a user leaves the organization.

Additionally, if their Role allows, authorized GEM server administrators can delete on-server recipients as well as any transitory records (e.g. unused uploads, templates, configurations, etc.) On-server data and configuration is backed up daily and can be configured to backup to an offboard customer storage location.

Software and Document Protection

All software deployed as part of the GEM Enterprise solution is digitally signed (including server, client, and mobile client software), and all are updated with new signatures at each release. All data entry points (including administrative, operations, employee portals, and automations) are protected against SQL injection attacks. Regular system log scans are conducted daily. Files are only managed by authorized and authenticated administrators and operators. The solution incorporates anti-virus protection to guard against inadvertent or malicious upload and distribution of unacceptable content.

Certifications

GEM Enterprise has been certified by the US Veterans Administration (TRM Certification). Also, both US and Canadian government and private enterprise customers run periodic penetration tests.

Genasys™

GEM Enterprise Audit Trails

Audit Trails

GEM Enterprise servers log every action taken by all individuals in reference to data/attributes functions, including user accesses, maintenance activities and configuration changes. Referential integrity is enforced so that all changes can be reviewed when necessary.

GEM Enterprise maintains detailed logs on:

i. System Administrator access to the application

ii. General operator/administrator access to the application

iii. Database maintenance activities

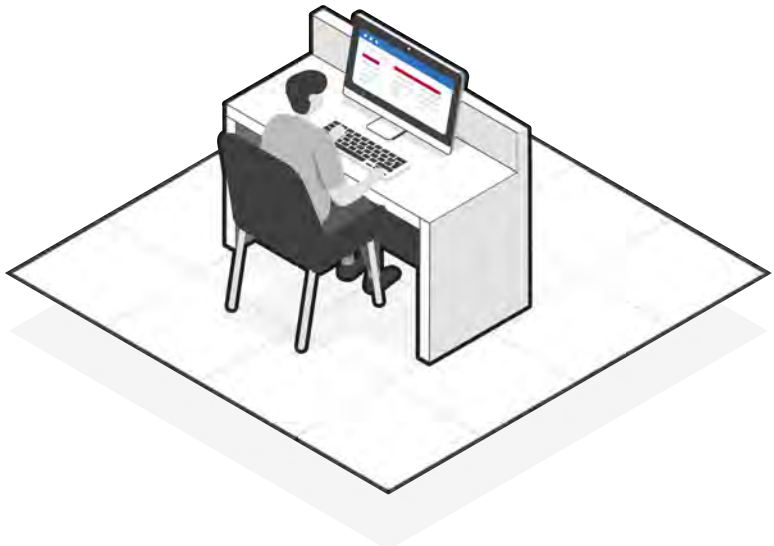
iv. Application configuration changes

The solution logs all user actions, which can be found in the "Console User Actions" section of the console.

All alert content is managed, with automatic archiving. Archives can be configured to periodically be moved from the server to an off-board customer storage environment.

Genasys Communications Canada Technical Support

GCC's R&D and Support staff receive Government of Canada background checks as part of receiving Reliability, Enhanced, and Secret clearance. Support staff are trained to be aware of privacy and security requirements, as well as customer-specific restrictions. Staff provide support by phone, email, conferencing, screen sharing and on-site if necessary. Full administrator and operator documentation is provided and instructor-led training courses are available.



Genasys™