MTS Echo® Security

MTS Echo Software

INTRODUCTION TO MTS ECHO SOFTWARE AS A SERVICE (SAAS)

MTS is committed to delivering Enterprise Class SaaS solutions that are lightweight, available 24x7x365, and protect customer data with the highest level of security. This document provides an overview of the secure infrastructure that supports the MTS Echo SaaS solutions, including:

- Physical Hosting and Networking
- Security
- Scalability
- Business Continuity / Disaster Recovery
- Change Management
- Monitoring
- Customer Support

PHYSICAL HOSTING AND NETWORKING

MTS Echo utilizes some of the most advanced technology for Internet security available today. MTS Echo solutions are hosted in Tier-3+ data center facilities, the highest rating available. MTS Echo is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders.

MTS employs Amazon Web Services (AWS) in multiple geographic regions and Availability Zones. AWS has a fully-redundant architecture and virtual connections that are maintained by Amazon web operations and infrastructure management experts. For more information, please see: http://aws.amazon.com/security/ and http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf. AWS features include:

NETWORK SECURITY

MTS employs industry best practices to ensure maximum security of customer data. As noted above, the MTS Echo infrastructure includes redundant firewalls, managed and monitored around-the-clock to monitor network traffic and safeguard systems and data from unauthorized access. To provide a further layer of security, a load-balanced Intrusion Detection System (IDS) analyzes all traffic for attack signatures and other anomalies and alerts support personnel of any suspicious activity for immediate follow-up. Since attack methods are constantly evolving, signatures are regularly updated on the IDS modules to enable the detection and prevention of new security threats. AWS security monitoring tools help identify denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks. Servers are hardened to turn off unnecessary services and proactive maintenance occurs on an ongoing basis to ensure all appropriate security patches are applied in a timely manner.

PHYSICAL SECURITY

» All areas are monitored 24x7x365 by archived closed-circuit CCTV digital cameras and armed security.
» Amazon data center are physically isolated and accessible only by highly trained AWS administrators.
» Access is restricted to authorized personnel through biometric two-factor authentication.

POWER AND ENVIRONMENT

» Redundant Continuous Power Supplies (CPS) and generator backups for all systems.
» Multiple Power Distribution Units (PDU) are used for preferred and backup source power.
» HVAC (Heating, Ventilation, Air Conditioning) systems arranged in an N+2 redundancy configuration.
» Controls provide appropriate levels of airflow, temperature and humidity.

FIRE DETECTION AND SUPPRESSION

» Multi-zoned, dry pipe, water-based fire suppression systems.
» Very Early Smoke Detection Alarm (VESDA) monitors to sample air and provide alarms prior to pressurization.
» Dual alarm activation necessary for water pressurization.

FLOOD CONTROL AND EARTHQUAKE PROTECTION

» Facilities are built above sea level with moisture barriers on exterior walls and no basement areas.
» Moisture detection systems and dedicated pump rooms for drainage/evacuation systems.
» Facilities meet or exceed requirements for local seismic building codes.

ADDITIONAL INFRASTRUCTURE FEATURES

» Redundant network connectivity to multiple Tier 1+ transit services.
» Redundant firewalls configured with session based fail-over.
» Redundant load balancers and core switch fabric.
» Load-balanced Intrusion Detection System (IDS).

DATA SECURITY

To protect data from eavesdroppers or any man in the middle attacks, MTS utilizes HTTPS along with the Transport Layer Security (TLS) protocol to encrypt and secure data in transit across the internet. Network and server level access is limited to authorized personnel only and is controlled through password and token two factor authentication. MTS applies the principles of role-based and least privileged access to all servers within the environment. Users are only granted privileges to access, read, write or execute within the servers and areas that apply to the specific duties of the individual.

Database servers are located behind a secondary firewall to further protect customer data from outside intrusion. MTS employs a single-tenant architecture within the database layer of the application. Each customer schema is separated to ensure there is no intermingling of customer data and that customers may not knowingly or unknowingly access data that does not belong to them.

Customers have the ability to add or remove user accounts through a special account administrator privilege. By default, only authorized users who have been added by the account administrator can access and view the equipment's status once logged in with their email and password. Administrators can revoke access for any user at any time.

MTS Echo transfers only the information that it needs to display the current status of the Test System so users can monitor their test and lab remotely. It does NOT transfer test data files or interact in any way with test data.

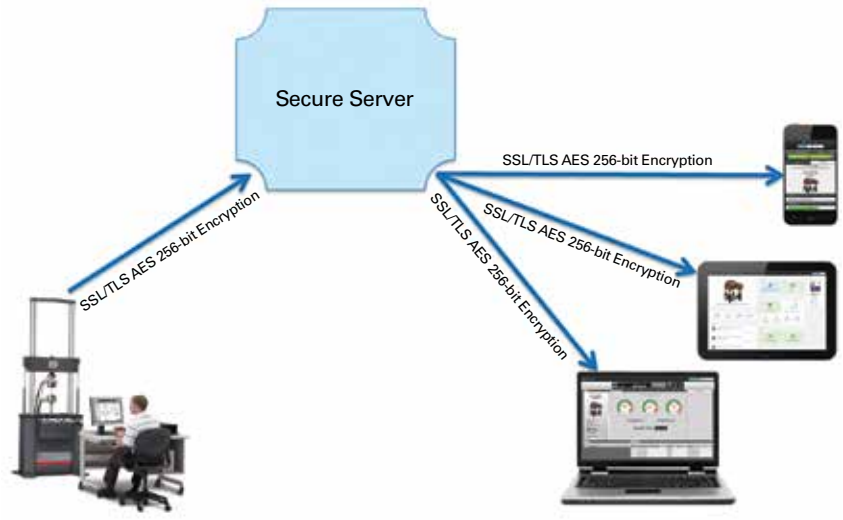
MTS Echo transfers only the following system status information:

» Test station Run State (Run, Hold, Stop)
» Test station Interlock State (On, Off)
» HPU and HSM Status (Off, Low, High)
» MTS 793 Controller information (Config Name, Controller Type, Build #, etc.)
» Current Signal Values Snapshot (Cycle Count, Runtime, Displacement, etc.)
  - Overwritten every time a new value is passed up to the secure server. Trends are not stored – only the current value is displayed.
» Station Manager Message Logs

Test data files are not accessible via MTS Echo. MTS data transfer is limited to receiving test status information. MTS Echo data files typically consist of customer authentication, lab test equipment and configured laboratory views.

COMMUNICATION SECURITY

All MTS Echo web communication is SSL/TLS AES 256-bit encrypted. Firewall ports are not required. The Controller PC controls when information is sent to the secure server. Only an outbound connection is established from the Controller PC to MTS Echo. The Controller PC sends status information to the secure server. Neither the secure server nor the MTS Echo enabled remote devices can initiate communications to the Controller PC. MTS Echo remote devices access a cached version of the test status information from the secure server.



CONTROLLER PC TO SECURE SERVER

» *Handshake and Encryption*
- Controller PC requests public key from server
- Server provides public key
- Controller PC generates and encrypts a symmetric encryption key with the public key
- Server decrypts handshake message with private key and obtains symmetric key
- From then on, the Controller PC encrypts messages with the symmetric key and the server decrypts them

» *Outbound Communication*
- The Controller PC sends encrypted status information outbound to the secure server
- The secure server has no way to send a message directly to that Controller PC – it is not able to get in through your firewall
- No firewall ports need to be opened
- Devices (smartphones, tablets, computers) viewing the status do not communicate with the Controller PC

» *Restricting HTTP Access*
- The Controller PC, or governing firewall, can be configured such that it only has access to mtsecho.com. All other web sites can be blocked.

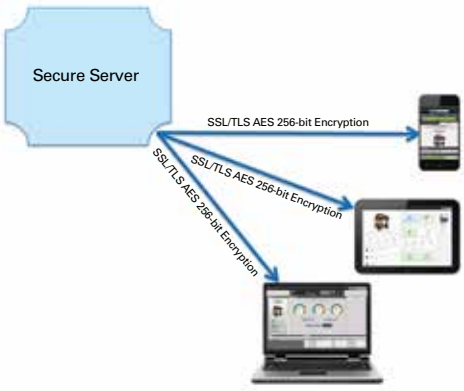
SECURE SERVER TO USER DEVICE

» *MTS Echo Interface*
- Users view the status of their Test System through the HTML5 MTS Echo Interface, Native Android or iPhone apps

» *Encryption*
- All communication between the Secure Server and User Devices is encrypted
- HTTPS certificate ensures login process is secure
- Customers may choose to use secure browsing (HTTPS) throughout the entire site

» *Restricted Access – 3 levels of configuration*
- By default, each user must login with their email and password before access is granted. A customer admin can remove access from any individual at any time.

» *Isolation from Controller PC*
- When a mobile device or browser loads the MTS Echo interface, it communicates with the Secure Server. All status shown is a cached version and served directly from the Secure Server. The MTS Echo interface does not connect directly to the Controller PC.



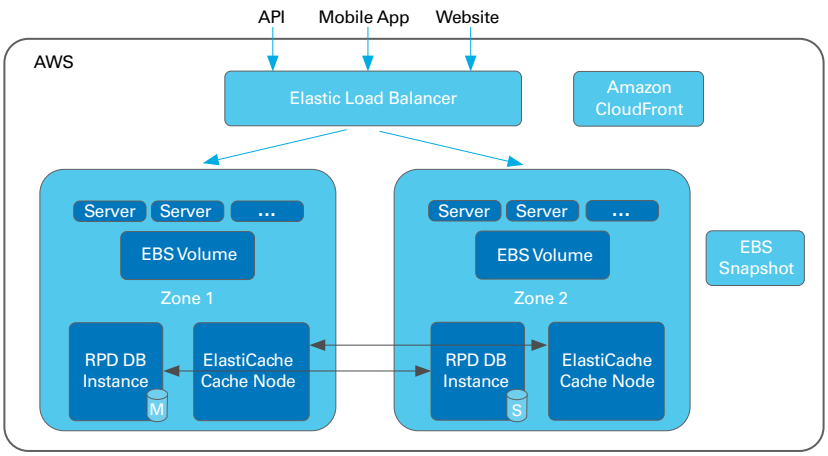
SCALABILITY

MTS Echo has been architected for maximum performance and scalability, allowing the application to remain robust and flexible enough to support an expanding customer base. The addition of virtual servers and other computing resources on an as-needed basis allows the fully fault-tolerant architecture to scale exponentially. Because of this scalability, customers are assured that their lab configurations are available to them at any time, regardless of the total number of simultaneous users.

SECURE SERVER INFRASTRUCTURE – BUILT FOR RELIABILITY AND SCALABILITY

MTS Echo secure server infrastructure is designed to provide robust uptime and scalability.

Elastic Load Balancing automatically distributes incoming application traffic across zones. Elastic Load Balancing automatically scales its request handling capacity to meet the demands of application traffic.



MTS Echo has two zones. Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone. MTS Echo is designed so that an entire Zone can go down without impacting the availability of the service.

Data is mirrored between zones so a zone can go down without impacting end users. Individual EC2 Servers scale according to real-time load to ensure bursts of traffic are handled without any impact on performance. Data is backed up automatically in an EBS Snapshot.

Finally, Amazon CloudFront uses a global network of edge locations, located near end users in the United States, Europe, Asia, and South America and Australia. MTS Echo utilizes CloudFront to deliver mobile app content with lower latency and high sustained data transfer rates to users all over the world.

BUSINESS CONTINUITY AND DISASTER RECOVERY

MTS Echo is hosted in Amazon's Tier 3+ data center facilities, built to withstand fires, floods and earthquakes and offer multi-level security, power systems with distributed redundancy, and environmental controls to provide optimum conditions for equipment operations. Despite having these capabilities for high-availability, in the event a data center is no longer operable, AWS maintains virtual server infrastructure at multiple independent, geographically separated locations for disaster recovery. With identically configured fail-over data centers, each with excess capacity and standby hardware, AWS is able to provide customers with disaster recovery. The maximum loss would be less than 24 hours as the most recent off-site back up recovery of authentication and lab configuration is restored.

MTS ECHO CHANGE MANAGEMENT

MTS employs a rigorous change management procedure that offers a comprehensive approach to addressing change planning, implementation, and follow-through in a manner consistent with ISO9001:2008 certification. This helps ensure quality customer support. It is essential that software changes are fully reviewed, tested and tracked so everyone who may be affected by a change is aware and in agreement.

The first step in implementing a software change is for the change request to be submitted in writing and a ticket created. After the request is submitted, the development team reviews the change and agrees upon any modifications to the change. Prior to implementation, the change is tested. It is then implemented and further tested on an alpha and beta instance of MTS Echo before it is placed into production.

MTS ECHO MONITORING AND SUPPORT

MTS Echo is monitored and supported 24x7x365. Integrated system, network, application and transaction monitoring tools check various performance and availability metrics continuously (such as CPU utilization, disk space and availability and URLs). Alerts are identified and resolved using issue resolution procedures. The MTS customer support teams have full access to service and technical support resources around the clock.

MTS Systems
14000 Technology Drive
Eden Prairie, MN 55344-2290 USA

Telephone: 1-952-937-4000
Toll Free: 1-800-328-2255

E-mail: info@mts.com
www.mts.com

ISO 9001 Certified QMS

MTS Echo Intelligent Lab can also be delivered through a local network solution with the MTS Echo Hub. Contact your Service Sales Engineer for more information.

100-306-386a EchoSecurity • Printed in U.S.A. • 09/21