MTS SmartService™ Security

Complimentary MTS SmartService tools help access important service information about test systems

INTRODUCTION

MTS is committed to delivering solutions that protect customer service history data with the highest level of security. This document provides an overview of the secure infrastructure that supports the MTS SmartService platform, including:

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

NEAR FIELD COMMUNICATION SECURITY

The MTS SmartService platform uses NFC chips embedded within an MTS SmartService sticker to tag equipment. No service history data is stored on this NFC chip beyond a unique identifier.

OFFLINE MODE SECURITY

The MTS SmartService customer tablet has an AirDrop-like feature that pairs with the MTS field service engineer's iPad to allow for a complete offline mode option (internet never allowed) while enabling support for firmware upgrades, software upgrades, and data backup. Uses Bluetooth Low Energy for device detection, secure Wi-Fi hotspot creation/connection, and communication via HTTPS over an industry standard 256-bit SSL-encrypted connection.

COMMUNICATION SECURITY

The customer tablet provides optional backup and updates setup using Wi-Fi capabilities and UI to enable networking functionality for security and control.

- Includes SSID search/connect/disconnect/forget features
- Supports WPA2, EAP, Guest Networks with captive portals, and HTTP proxy settings
- Back up and updates performed over industry standard 256-bit SSL-encrypted connection
- Communication is SSL/TLS AES 256-bit encrypted
- Firewall ports not required
- MTS SmartService tablet controls when service history data is transferred for backup

SERVICE HISTORY DATA SECURITY

To protect service history data from eavesdroppers or any man in the middle attacks, MTS uses 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 service history data from outside intrusion and we employ sophisticated fraud detection algorithms to identify and lock access immediately. Furthermore, customer service history data is encrypted at rest using AES 256-bit encryption.

NETWORK SECURITY

MTS SmartService employs industry best practices to ensure maximum security of customer service history data. The MTS SmartService infrastructure includes redundant firewalls, managed 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.

Amazon Web Services (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 centers 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).

SECURE INFRASTRUCTURE – BUILT FOR RELIABILITY AND SCALABILITY

MTS SmartService secure infrastructure is designed to provide robust uptime and scalability. Load balancing automatically distributes incoming backup traffic across zones, and scales request handling capacity to meet the demands of traffic.

MTS SmartService uses at least 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 SmartService is designed so that an entire zone can go down without impacting the availability of the service. Infrastructure scales according to real-time load to ensure bursts of traffic are handled without any impact on performance.

PHYSICAL HOSTING AND NETWORKING

MTS SmartService uses some of the most advanced technology for security available today. It is hosted in Tier-3+ data center facilities that have the highest security rating.

MTS employs 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.

BUSINESS CONTINUITY AND DISASTER RECOVERY

MTS SmartService 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 SMARTSERVICE CHANGE MANAGEMENT

MTS SmartService 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 SmartService before it is placed into production.

MTS SMARTSERVICE MONITORING AND SUPPORT

MTS SmartService is monitored and supported 24x7x365. Integrated system, network, and transaction monitoring tools check various performance and availability metrics continuously (such as CPU utilization, disk space and availability). 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

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

Telephone: 1-952-937-4000
Toll Free: 1-800-328-2255
Fax: 1-952-937-4515

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

ISO 9001 Certified QMS

100-479-657 SmartServiceSecurity • Printed in U.S.A. • 3/19