Trusted Manager (TMAN)

Supported File Types

Providing high-speed, secure information sharing for modern military, intelligence, and law enforcement

Trusted Manager (TMAN) is a multi-level security (MLS) cross-domain intelligence sharing solution. TMAN provides a secure platform for transferring approved file types and streaming data to and from networks operating at different security classifications. Security requirements are enforced in accordance with Director of Central Intelligence Directive (DCID) 6/3 standards. TMAN is currently accredited by the Air Force Intelligence Surveillance and Reconnaissance Agency (AFISRA) and is listed on the United Cross Domain Management Office (UCDMO) Cross Domain Inventory.

TMAN is a Lockheed Martin product created and maintained by a dedicated team of developers, testers, information assurance personnel, field specialists, and trainers. The TMAN team has a proven track record in customer satisfaction with successful site installations, hands-on training, and mission support. TMAN systems and professional services are available on the General Services Administration Advantage ® website at www.gsaadvantage.gov.

Supported File Types

TMAN only permits messages with known formats to cross the source/destination boundary. Each site is explicitly authorized and accredited to accept a sub-set of these supported file formats. TMAN enforces strict policies and rules for each of the supported file types:

NITF 2.0/2.1

National Imagery Transfer Format (NITF) files are NITF Standard per MIL-STD 2500A to MIL-STD 2500C. Each NITF file is validated according to the standards, embedded sensitivity labels, and optional geographic filtering.

Office Files

TMAN provides an in-depth inspection for “hidden data” in Microsoft® Word, Excel®, and PowerPoint® documents. “Hidden data” refers to information made invisible or concealed in a document un-intentionally or intentionally. TMAN inspects documents for various items by following the policy defined for each file type and the action being performed on the file. TMAN applies separate policies for both automatic review for upgrade and reliable review for downgrade.

Additional File Types

TMAN supports many additional formats including XML, text-based files, video clips, imagery, mission data, weather, map data, and more.

Imagery and Graphics
.ntf, .aip, .mti, .hdf
.complex, .saip_complex
.mimic, .vitec
.bmp, .emf
.jpg, .png
.gif, .tif, .tiff
Mission Data
.aco, .ato, .actm, actdf,
.dbf, .dbu, eid, .eob
.trep, .tgt, .spl
.grb, .iads
Text
.txt, .csv, .dif, .tab, .pdf
Markup Documents
.xml, .html, .kml, .xhtml
Video
.mpg, .mp1, .mp2, .mp4
.m2v, .ts, .avc

Office files
.ppt, .pptx, .pps, .ppa, .pot
.xls, .xlsx
.doc, .docx, .dot
.adp, .rtf
.mda, .mdb, .mde, .mdw
Audio
.wav, .mp3, .mp4
DAFIF
.ID, .prj, .shx, .shp, .dat
Other
.hdf
.info
.cdc, .crd, .crc (XML)
.TT
.eps

LOCKHEED MARTIN

Trusted Security Solutions (TSS)

*** TMAN products may be/are subject to the controls of the U.S. Department of State**

Version 3.8 Revision 05/2013

File-Based Data Transfer

DoD Photo Archive/Master Sgt. Desiree N. Palacios

TMAN supports multiple modes of source-to-destination file transfer, including File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), SFTP with Secure Copy (SCP), File Transfer Protocol over SSL (FTPS), and Network File System (NFS). TMAN is configurable to either pull or received files and supports multiple concurrent connections.

TMAN leverages Public Key Infrastructure (PKI) concepts, including digital signatures and public/private key pairs. For downgrade, files are digitally signed before they are sent to TMAN. The use of digital signatures provides Authentication, Non-Repudiation, and Integrity.

All incoming files are validated upon receipt. Files that are successfully validated are disseminated to the destination-side. Files that fail validation are diverted to a problem queue for administrative evaluation and resolution. All file transactions are journaled, logged, and audited, providing a complete record of events.

Security Measures

The TMAN system provides multiple layers of protection for Defense in Depth: the TMAN Server, the IP Filter Firewall, and the Screening Router. The system further protects information be leveraging Mandatory, Discretionary, and Role-Based Access Controls.

TMAN Server

The TMAN server is an application-level guard running Solaris 10 with Trusted Extensions on the x86 platforms. These platforms provide TMAN with the capability to securely process data at multiple classification levels. All messages must stop and start at the TMAN server, which validates, virus scans, and packet-filters messages before sending them to the authorized enclaves.

IP Filter Firewall

The TMAN system uses IP Filter firewall software to filter data traffic at the system interface. This second layer of protection further ensures the security of trusted information.

The Screening Router

Essentially, the screening router is used as a packet-filtering firewall. The screening router is a switching router that provides access control based on the source IP address, destination IP address, and destination port number. Only the pre-approved combinations of IP address, port number, and transport type pass through the screening router to the TMAN system.

Access Control

Access to the TMAN management interface is gained through local login. Each user is given a unique username and password defined by rigid criteria then assigned roles and responsibilities for configuration and maintenance. Role Based Access Control (RBAC) is enforced for all privileged TMAN accounts, providing users with only the necessary capabilities defined by their role.

Integrity Checking and Audit Reporting

TMAN implements an integrity checker and Basic Audit Reporting Tool (BART) to check critical system files for changes. Security relevant files, TMAN code, and operating system files are checked for any alterations.

Modes of Operation

All incoming files, intended for upgrade or downgrade, encounter a verification and scanning process enabled on the system. However, not all files require human review, but use the system's scanning and verification capabilities to ensure security.

Automatic Review for Upgrade	Approved data types are validated, virus scanned, and transported to an enclave of user-designated higher classification.
Human Reliable Review	Approved data types are validated and presented for human review; upon which, the human reviewer approves the downgrade or disapproves the downgrade.
Automatic Review for Downgrade	Data is automatically reviewed and released to an enclave of a lower classification. TMAN verifies the security level of the submitted data by checking the accompanying metadata. Additionally, TMAN may scan metadata for geographic constraints.

Trusted Manager
1300 S Litchfield Rd, MS 1411
Goodyear, AZ 85338
Phone: 866-500-TMAN
Info: TMAN.info@lmco.com

Program Area Manager
Steve Bean
steve.bean@lmco.com
623-925-7508

Engineering Program Manager
Linda Brady
linda.brady@lmco.com
623-925-7031