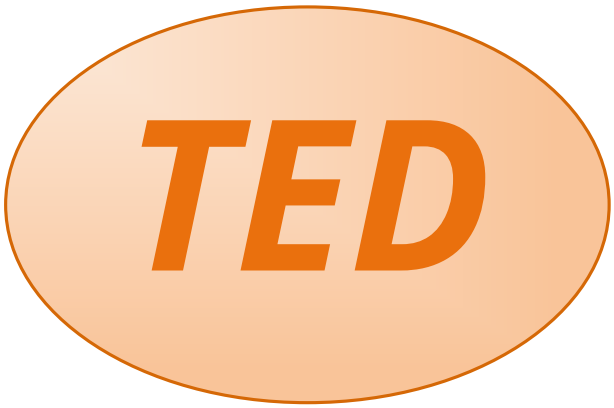
TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

DYNAMIC SYSTEMS' TED RESTORES DESKTOP FUNCTIONALITY FOR SOLARIS 11.4 TRUSTED EXTENSIONS

Solaris 11.4 Trusted Extensions (TX) is a powerful security technology that allows the creation of a multilevel (labeled) security environment in which users with different access permissions can work simultaneously with data that has discrete access control requirements. This enables strict access control enforcement for data based on both data sensitivity and data ownership.

With the Desktop for Solaris TX provided by the Dynamic Systems' Trusted Extensions Desktop (TED), Solaris 11.4 regains the multilevel desktop that was used in 11.3 and other, previous Solaris versions. User accounts can be configured to see only their individual allowed labels. TED controls ensure that data labeled by TX is only visible/accessible in an appropriately labeled window. TX and TED default controls prevent data movement between labels. Additionally, if desired, each label can be configured to require a separate password. Using TED, users who are authorized to view data at multiple classification levels can do so on a single desktop, with separation of information still strictly enforced.



TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

Extends Solaris 11.4 Security

Maintains data separation in processing, at rest, and in transit

Enforces user and process rights management

Mandatory Access Control

MAC policy adds sensitivity labels

Data visibility constrained within labels

Labeled Desktops

Users who are authorized to view data at multiple sensitivity levels can do so on a single desktop, with data separation still strictly enforced

Labeled Device Access

File Systems
Terminals
HDD | SSD
CD | DVD
USB Drives
Printers
Audio Devices

Labeled Networks

Secured data exchange between multiple systems

Preserves label security when sharing data via NFS or other network protocols

Secured Environments

Commercial
Government
DoD

Non-Hierarchical and Hierarchical data separation

What's New in Solaris 11.4?

In version 11.4, standard Solaris supports file and process labeling using the same labeling APIs and CLIs as Trusted Extensions. The labeling syntax is now the same in both standard Solaris and Trusted Extensions, and the new *labelcfg* command can be used to configure labels in both environments.

However, in version 11.4, the way that label policy is enforced is very different between standard Solaris and Trusted Extensions. As an example: standard Solaris permits writing down to lower labeled objects, Trusted Extensions, by default, does not.

Likewise, the application of labels is different.

- TX applies labels to zones and network endpoints
- Standard Solaris applies labels to System V IPC objects

Additionally, while both environments support individual file labeling in ZFS, the labeling policy differences prevent the sharing of labeled file systems between standard Solaris and TX.

Finally, potentially the largest impact to current TX users, **Solaris 11.4 Trusted Extensions no longer provides a multilevel desktop** (Trusted Desktop).

TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

Trusted Desktop for Solaris Trusted Extensions

TED Overview

Dynamic Systems' Trusted Extensions Desktop restores multilevel desktop functionality to Solaris 11.4. TED provides the same functionality as the Solaris 11.3 Trusted Desktop does for 11.3 Trusted Extensions. TED maintains the label-based security policy and policy enforcement while also maintaining system and security administration procedures.

TED restores the 'single-pane-of-glass' user capability to Solaris 11.4 Trusted Extensions. TED allows a user to open multiple labeled windows on a single desktop. TED keeps data separated per label while providing user access to each labeled environment. A single single-pane-of-glass / user desktop can be one or more physical monitors configured to function as a single desktop.

New Solaris 11.4 Features – TED incorporates Solaris 11.4 enhanced security functionality which benefits Solaris TX customers. With Solaris 11.4, the customer gets: Instantaneous ZFS Copy of files and directories (via cloning and copy-on-write) – Explicit and automatic individual file labeling – Per-file auditing for local and NFS file systems – Administrative Command History – Web-based Solaris Account Manager – OpenLDAP automation – Label Encodings Configuration Tool.

Policy Enforcement – TED uses two primary policy enforcement mechanisms. User-based policy is defined via Role-Based Access Control (RBAC). Service-based policy is defined using the Service Management Facility (SMF). Both frameworks leverage process rights management (privileges) which are interpreted by the kernel to grant or deny access to protected resources.

Data Access – Users access each environment through a labeled window but can only move data as configured in Trusted Extensions.

TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

Multi-Sensitivity Level Architecture – Solaris TX Layered Architecture implements mandatory access control, hierarchical labels, 'least privilege' access principle, secured pathing, and role-based access controls.

TED Security Support

Trusted Extensions Desktop restores multilevel desktop functionality to Solaris 11.4. TED provides patched versions of the X11 and Xvnc servers that have been extended to enforce the multilevel security policies that were previously provided in Solaris 11.3. Consequently, TED is compliant with Oracle's Solaris 11.4 security hardening guidance. Solaris 11 STIGs remain 100% in effect with the TED build.

The TED Trusted Desktop is based on the MATE desktop environment. MATE is an open source continuation of the GNOME2 desktop environment, but uses the 64-bit GTK+3 libraries so it is completely compatible with the Solaris 11.4 GNOME3 applications. Best practice security guidelines for GNOME will be followed to the extent possible for MATE.

TED Factory Security Assessment – Dynamic Systems assesses TED security compliance using the Security Content Automation Protocol (SCAP) benchmarks for Solaris 11. Additionally, the build environment is assessed using a vulnerability scanner.

TED Support for Customer Assessment – Delivery of the TED package comes with both documentation and engineering to support the customer's successful security assessment and receipt of ATO.

TED is installed onto an unmodified Solaris 11.4 Operating System instance using the Solaris Image Packaging System (IPS). It is configured and updated using the same administrative procedures as were utilized with Solaris 11.3.

TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

With the TED enhancement, the 11.4 OS is assessed for security compliance following standard security guidelines. Dynamic Systems recommends that TED be assessed as an application inside of Solaris 11.4.

The TED Systems Security Plan (SSP) documents applied security controls supporting customer ATO. The TED SSP provides a description of all security controls and how each control is implemented. Technical descriptions are provided for each TED interface to include information required for the customer's Secure Protocols Identification document.

TED Product Support

Build Delivery – TED initial build provides a hardened TED instance for installation on a customer Solaris 11.4 instance. The TED Installation Guide includes detailed installation instructions and provides an SSP that documents the requisite security controls as needed for successful customer security assessment.

TED provides three delivery mechanisms. The customer can – pull the TED packages and instruction set from the Dynamic Systems TED repository – request that the TED team drop the repository and instruction set on their secure drop point – or, request a media based copy.

TED offers two Initial Build options – Standard & Premium. For both, the customer obtains the TED delivery package as described. The standard and premium options provide different levels of TED engineering install support.

Sustainment – TED provides a single source for patches and updates. The TED engineering team monitors all relevant sources and accumulates system and security patches – as well as system updates – from all sources and provides a single cumulative quarterly patch release to customer system administrators. Each patch/update comes with installation instructions and an updated SSP.

TRUSTED EXTENSIONS DESKTOP

DYNAMIC SYSTEMS INC

TED offers two Sustainment options – Standard and Premium. Both provide the customer with patches, updates, and engineering/troubleshooting support. The standard and premium options provide different levels of TED engineering sustainment support.