Safe Update

DATASHEET (iSecurity Suite Network Protection)

Regulate File Editors in Production Environments

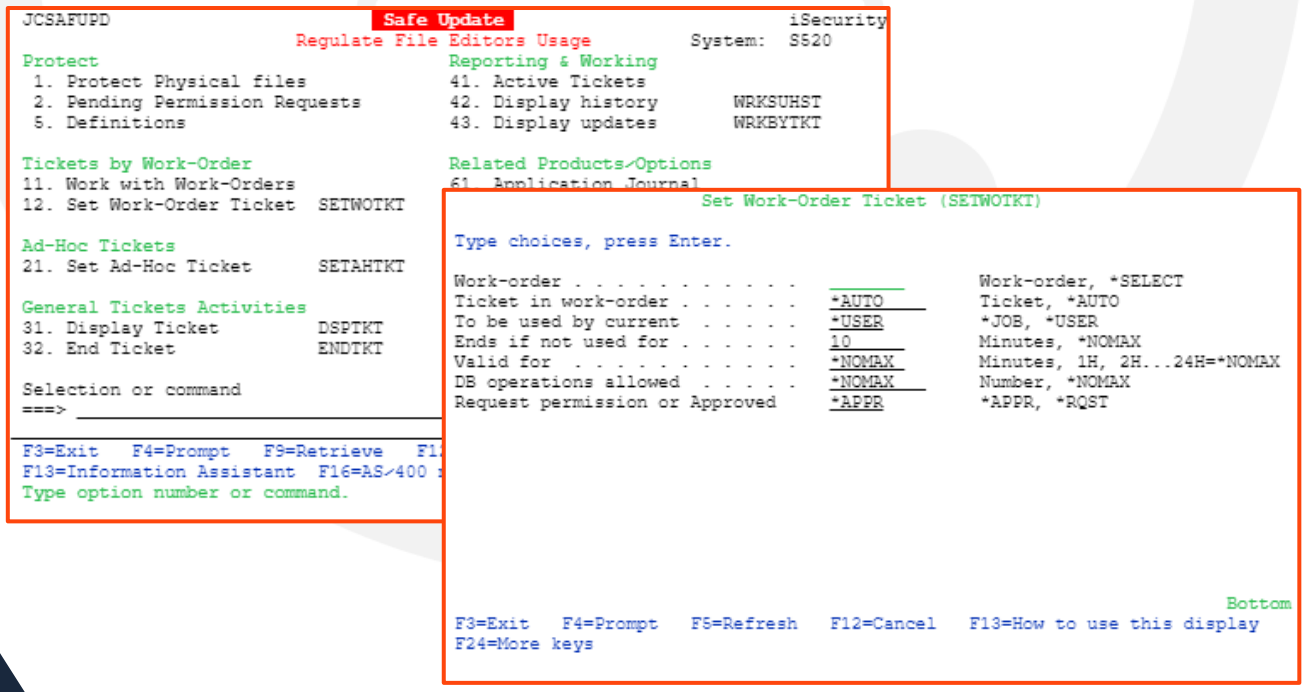
Security systems that protect data by preventing the access of programmers to production environments are not enough. Occasionally programmers need to conduct some missions and temporarily get *ALLOBJ authority. As there is no way to restrict them to that mission, they became a potential risk.

iSecurity Safe-Update's new security layer ensures that only authorized programs are used to update business critical files.

Safety on Production Environment with iSecurity Safe Update

When the organization needs to update data with normally not allowed tools. Some users are stubborn about using the tools allowed by IT Departments, and this "Shadow IT" is always a risk.

- iSecurity Safe-Update implements a workflow that consists of work orders, that specify who can work with the data, the reason for the work, and the limited time during which the work order is valid.
- If an unauthorized update is attempted, a window appears requesting the entry of a ticket.



Key Features

- Allows authorized users to create ad-hoc tickets, which are tracked in the same way as work orders.
- Work orders specify the programmer, the files, the updates required and the time frame.
- Tickets are automatically closed if inactive for a period of time.
- Allows updates to fields that are marked as insignificant.
- Subject to the organization policy, ad-hoc tickets might be permitted as well.
- Creates a record of updates, logging who updated the data, who authorized the update, and why it was done.
- Database journal information displayed by **AP-Journal** commands highlights updates made under Safe-Update permissions.

iSecurity Safe Update Benefits

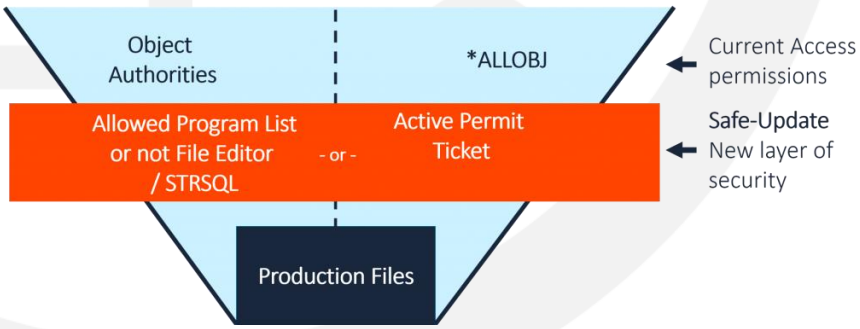
- Monitors and protects updates to data according to the program used.
- Uses either a whitelist of allowed programs, or a blacklist of programs that are not allowed.
- Ensures that DFU, Start SQL and file editors are not used in production environments even when *ALLOBJ is in effect.
- Restriction of updates can be removed when the update is only for field marked in advance as “insignificant”.
- Programs that may not update data can read it. They will be stopped when an update is issued.
- Comprehensive workflow of management-approved work orders with tickets opened by preassigned programmers.

Adding a New Security Layer

iSecurity Safe-Update implements a workflow that consists of work orders, created by management, that specify who can work with the data, the reason for the work, and the limited time during which the work order is valid.

Based on the work order, the specified programmer can then open a ticket and perform the requested updates interactively or in batch. All work under the tickets is logged, even if the data files themselves are not journaled.

If an unauthorized update is attempted, a window appears requesting the entry of a ticket.



Let’s Get Started

Schedule your Demo and start using Network Protection on your Systems with iSecurity Safe Update.

RAZ-LEE iSecurity