

---

# I-0414: Method Of Audit Prevention May Be Site-Configurable

---

TYPE: NIAP Interpretation  
NUMBER: I-0414  
STATUS: Posted for External Review

TITLE: Method Of Audit Prevention May Be Site-Configurable  
WOULD SUPERSEDE: [I-0348](#)  
COMMENTS DUE BY: Tuesday, May 29, 2001 to [IWG@gibraltar.ncsc.mil](mailto:IWG@gibraltar.ncsc.mil)

SOURCE REFERENCE: CC v2.1 Part 2 Subclause 3.6 FAU\_STG  
CC v2.1 Part 2 Subclause C.6 FAU\_STG

RELATED TO: [I-0348](#) Audit Data Loss Prevention Method May Be Site-Selectable

## ISSUE:

The FAU\_STG family does not support a way for the administrator to specify that the actions taken by the TSF to prevent audit data loss when the audit trail is full can be site-selectable. Instead, the FAU\_STG.4.1 element explicitly states the actions to be taken by the TSF when the audit log is full. This wording implicitly prevents a site from selecting the actions taken to prevent loss of audit data.

## STATEMENT

It is acceptable for the TSF to allow the method taken by the TSF to prevent audit loss when the audit trail is full to be site-selectable, as long as the TSF provides a pre-determined set of allowable actions and one of these actions is defined as a default.

## SPECIFIC INTERPRETATION:

To address this interpretation, the following changes are made to CC v2.1: (additions marked thusly; deletions marked ~~thusly~~)

- In Clause 3, Figure 3.1, the component levelling diagram for FAU\_STG is modified to show a new component, NIAP-0414, that is hierarchically above component 4.
- In Subclause 3.6, the component levelling diagram is modified to show a new component, NIAP-0414, that is hierarchically above component 4.
- In Subclause 3.6, the following paragraph is added after paragraph 129:

FAU\_STG.NIAP-0414 Site-Configurable Prevention of Audit Loss permits the site to determine the action to be taken when the audit trail is full.

- In Subclause 3.6, the following is added after paragraph 133:

**Management: FAU\_STG.NIAP-0414**

The following actions could be considered for the management functions in FMT:

1. Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.

- In Subclause 3.6, the following is added after paragraph 136:

**Audit: FAU\_STG.NIAP-0414**

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

1. Basic: Actions taken due to the audit storage failure.
  2. Basic: Selection of an action to be taken when there is an audit storage failure.
- The following component is added to Subclause 3.6, FAU\_STG, after FAU\_STG.4:

#### **FAU\_STG.NIAP-0414 Site-Configurable Prevention of Audit Loss**

**Hierarchical to:** FAU\_STG.4

**FAU\_STG.NIAP-0414-1.** The TSF shall provide the administrator the capability to select one or more of the following actions [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*] to be taken if the audit trail is full.

**FAU\_STG.NIAP-0414-2.** The TSF shall [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full and no other action has been selected.

#### **Dependencies:**

- FAU\_STG.1 Protected Audit Trail Storage
- FMT\_MTD.1 Management of TSF Data
- In Clause C, Figure C.1, the component levelling diagram for FAU\_STG is modified to show a new component, NIAP-0414, that is hierarchically above component 4.
- In Subclause C.6, FAU\_STG, the following is added after paragraph 640:

#### **FAU\_STG.NIAP-0414 Site-Configurable Prevention of Audit Loss**

##### **User Application Notes:**

This component specifies the set of administrator selectable actions that the TSF must be capable of performing when the audit trail is full and allows the administrator to specify which action is to be performed by the TSF. It also provides a default action to take if the administrator does not select one of the actions.

##### **Operations**

##### **Selection:**

In FAU\_STG.NIAP-0414-1, the PP/ST author should select one or more of the following actions that the TSF must have the ability to perform: (1) ignore auditable actions, (2) prevent the occurrence of auditable actions, and (3) overwrite the oldest audit records.

In FAU\_STG.NIAP-0414-2, the PP/ST author should select one of the actions as the default action to be performed by the administrator in the event that no action is selected by the administrator.

##### **Assignment:**

In FAU\_STG.NIAP-0414-1, the PP/ST author should specify other actions that should be taken in case of audit storage failure, such as informing an authorized user.

In FAU\_STG.NIAP-0414-2, the PP/ST author should specify other actions that should be taken in case of audit storage failure when no action has been selected, such as informing the authorized user.

## **PROJECTED IMPACT:**

Negligible impact anticipated.

## **SUPPORT:**

A new component is required that allows a site to select the action(s) to be performed by the TSF when the audit trail is full. This ability increases the flexibility of the TOE and allows the TOE to adjust to changing security needs.

This new component also specifies the default action(s) to be taken if no action is selected by the administrator.

Note 1: The management section for FAU\_STG.4 implies that site-selectable actions are permitted. This statement is inconsistent with FAU\_STG.4.1, which requires the PP/ST author to explicitly select and assign the actions to be taken when the audit trail is full.

Note 2: FAU\_STG.4 refers to "the authorised user with special rights". This phrase is not defined and is not used elsewhere in the Common Criteria. In addition, this interpretation describes the "administrator" as the one selecting the action performed by the TSF when the audit trail is full, and "the authorized user with special rights" is notified when the audit trail fills up. Although it introduces an internal inconsistency in the interpretation, the phrase was used to be consistent with the wording of FAU\_STG.4.