

Audit Requirements

Natural language input for SFRs

In order to assure that information exists that allows Security Administrators to discover intentional and unintentional issues with the configuration and/or operation of the system, compliant TOEs have the capability of generating audit data targeted at detecting such activity. Auditing of administrative activities provides information that may hasten corrective action should the system be configured incorrectly. Audit of select system events can provide an indication of failure of critical portions of the TOE (e.g., a cryptographic provider process not running) or anomalous activity (e.g., establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the system) of a suspicious nature.

In some instances there may be a large amount of audit information produced that could overwhelm the TOE or administrators in charge of reviewing the audit information. The TOE must be capable of sending audit information to an external trusted entity, which mitigates the possibility that the generated audit data will cause some kind of denial of service situation on the TOE. This information must carry reliable timestamps, which will help order the information when sent to the external device.

Loss of communication with the audit server is problematic. While there are several potential mitigations to this threat, this cPP does not mandate that a specific action takes place; the degree to which this action preserves the audit information and still allows the TOE to meet its functionality responsibilities should drive decisions on the suitability of the TOE in a particular environment.

Proposed SFRs

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the *not specified* level of audit; and
- c) *All administrative actions;*
- d) *Specifically defined auditable events listed in Table 1.*

Application Note: The term 'administrative actions' comprises:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).

- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Changing passwords (name of related user account shall be logged).
- Starting and stopping services (if applicable)
- Other uses of privileges.

Application Note: The ST author can include other auditable events directly in the table; they are not limited to the list presented.

Assurance Activity (taken from NDPP with only minor changes):

The evaluator shall check the guidance documentation and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by this cPP is described and that the description of the fields contains the information required in FAU_GEN1.2, and the additional information specified in Table 1.

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this cPP. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in this cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security relevant with respect to this PP. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in table 1 and administrative actions listed above. This should include all instances of an event--for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *specifically defined*

auditable events listed in Table 1.

Assurance Activity:

This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.

Table 1 Network Devices.

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|--|--|
| FAU_GEN.1 | None. | None. |
| FAU_GEN.2 | None. | None. |
| FAU_STG_EXT.1 | None. | None. |
| FCS_CKM.1 | None. | None. |
| FCS_CKM_EXT.4 | None. | None. |
| FCS_COP.1(1) | None. | None. |
| FCS_COP.1(2) | None. | None. |
| FCS_COP.1(3) | None. | None. |
| FCS_COP.1(4) | None. | None. |
| FCS_RBG_EXT.1 | None. | None. |
| FDP_RIP.2 | None. | None. |
| FIA_PMG_EXT.1 | None. | None. |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism. | Provided user identity, origin of the attempt (e.g., IP address). |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None. | None. |
| FMT_MTD.1 | None. | None. |
| FMT_SMF.1 | None. | None. |
| FMT_SMR.2 | None. | None. |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_STM.1 | Changes to time. | The old and new values for the time. Origin of the attempt (e.g., IP address). |
| FPT_TUD_EXT.1 | Initiation of update and result of the update attempt (success or failure) | No additional information. |
| FPT_TST_EXT.1 | None. | None. |
| FTA_SSL_EXT.1 | Any attempts at unlocking of an interactive session. | |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | |
| FTA_SSL.4 | The termination of an interactive session. | |
| FTA_TAB.1 | None. | None. |
| FTP_ITC.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | |
| FCS_IPSEC_EXT.1 (only if IPSEC is supported/selected) | Failure to establish an IPsec SA. | Reason for failure |
| FCS_TLS_EXT.1 (only if TLS) | Failure to establish a TLS | Reason for failure |

| | | |
|---|---------------------------------------|--------------------|
| is supported/selected) | Session | |
| FCS_SSH_EXT.1 (only if SSH is supported/selected) | Failure to establish an SSH session | Reason for failure |
| FCS_HTTPS_EXT.1 (only if HTTPS is supported/selected) | Failure to establish a HTTPS Session. | Reason for failure |
| FPT_ITT.1(1) | None | None |
| FPT_ITT.1(2) | None | None |

Table 1 Firewalls

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|--|--|
| FAU_GEN.1 | None. | None. |
| FAU_GEN.2 | None. | None. |
| FAU_STG_EXT.1 | None. | None. |
| FCS_CKM.1 | None. | None. |
| FCS_CKM_EXT.4 | None. | None. |
| FCS_COP.1(1) | None. | None. |
| FCS_COP.1(2) | None. | None. |
| FCS_COP.1(3) | None. | None. |
| FCS_COP.1(4) | None. | None. |
| FCS_RBG_EXT.1 | None. | None. |
| FDP_RIP.2 | None. | None. |
| FIA_PMG_EXT.1 | None. | None. |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism. | Provided user identity, origin of the attempt (e.g., IP address). |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None. | None. |
| FMT_MTD.1 | None. | None. |
| FMT_SMF.1 | None. | None. |
| FMT_SMR.2 | None. | None. |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_STM.1 | Changes to time. | The old and new values for the time. Origin of the attempt (e.g., IP address). |
| FPT_TUD_EXT.1 | Initiation of update and result of the update attempt (success or failure) | No additional information. |
| FPT_TST_EXT.1 | None. | None. |
| FTA_SSL_EXT.1 | Any attempts at unlocking of an interactive session. | |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | |
| FTA_SSL.4 | The termination of an interactive session. | |
| FTA_TAB.1 | None. | None. |
| FTP_ITC.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | |
| FCS_IPSEC_EXT.1 (only if IPSEC is supported/selected) | Failure to establish an IPsec SA. | Reason for failure |

| | | |
|---|---------------------------------------|--------------------|
| FCS_TLS_EXT.1 (only if TLS is supported/selected) | Failure to establish a TLS Session | Reason for failure |
| FCS_SSH_EXT.1 (only if SSH is supported/selected) | Failure to establish an SSH session | Reason for failure |
| FCS_HTTPS_EXT.1 (only if HTTPS is supported/selected) | Failure to establish a HTTPS Session. | Reason for failure |
| FPT_ITT.1(1) | None | None |
| FPT_ITT.1(2) | None | None |

FAU_GEN.2 User identity association

Hierarchical to: FAU_GEN.1 Audit data generation

Dependencies: FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Assurance Activity:

This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.

FAU_STG_EXT.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit date to an external IT entity using a trusted channel implementing the [selection: IPsec, SSH, TLS, TLS/HTTPS] protocol.

Application Note:

For selecting the option of transmission of generated audit date to an external IT entity the TOE relies on a non-TOE audit server for storage and review of audit records. The storage of these audit records and the ability to allow the administrator to review these audit records is provided by the operational environment in that case.

In the second selection, the ST author chooses the means by which this connection is protected. The ST author also has to ensure that the supporting protocol requirement matching the selection is included in the ST.

Assurance Activity:

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall also examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the

TOE needed to communicate with the audit server. The evaluator shall perform the following test for this requirement:

- Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

Application Note: The local space to store audit data is limited. The TSF shall generate a warning to inform the user before the local space to store audit data is used up and/or the TOE will lose audit data due to insufficient local space.

Assurance Activity:

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server (for TOEs that are not acting as an audit log server). For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. If the TOE complies with FAU_STG_EXT.1.4 the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.1.4 are correct.

FAU_STG_EXT.1.3 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] when the local storage space for audit data is full.

Application Note: The external log server might be used as alternative storage space in case the local storage space is full. The 'other action' could in this case be defined as 'send the new audit date to an external IT entity'.

Assurance Activity:

This activity should be accomplished in conjunction with the testing of FAU_STG_EXT.1.2.

The evaluator shall examine the TSS to ensure that it details the behavior how the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen like sending the new audit date to an external IT entity as given as example in the Application Note above, the related behavior of the TOE shall also be detailed in the TSS. The evaluator shall also ensure that the guidance documentation describes all possible configuration options and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

Optional:

FAU_STG_EXT.1.4 The TSF shall provide information about the number of [selection: dropped, overwritten, assignment: other information] audit records in the case where the local storage has been filled and the TSF takes one of the actions defined in FAU_STG_EXT.1.3.

Application Note:

This option should be chosen if the TOE supports this functionality. In case the local storage for audit records is cleared by the administrator, the counters associated with the selection in the SFR should be reset to their initial value (most likely to 0).

Assurance Activity:

This activity should be accomplished in conjunction with the testing of FAU_STG_EXT.1.3.

The evaluator shall examine the TSS to ensure that it details the possible options the TOE supports for information about the number of audit records that have been dropped, overwritten, etc in case the local storage for audit data is full. The evaluator shall also ensure that the guidance documentation describes all possible configuration options and the meaning of the result returned by the TOE for each possible configuration. The description of possible configuration options and explanation of the result shall correspond to those described in the TSS.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application Note: The TSF do not provide reliable information about the current time at the TOE's location by themselves, but depend on external time and date

information, either provided manually by the administrator or through the use of an NTP server. The term 'reliable time stamps' refers to the strict use of the time and date information, that is provided externally, and the logging of all changes to the time settings including information about the old and new time. With this information the real time for all audit data can be calculated.

Assurance Activity:

The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time. The TSS provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.

- Test 1: The evaluator uses the guidance documentation to set the time.

The evaluator shall then use an available interface to observe that the time was set correctly.

- Test2: [conditional] If the TOE supports the use of an NTP server; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple cryptographic protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol.

(optional) FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(1)/Audit: The TSF shall restrict the ability to *determine the behaviour of, modify the behaviour of the functions transmission of audit data to an external IT entity to authorized administrators.*

FMT_MOF.1(2)/Audit: The TSF shall restrict the ability to *determine the behaviour of, modify the behaviour of the functions handling of audit data to authorized administrators.*

Application note:

FMT_MOF.1(1)/Audit should only be chosen if the transmission protocol for transmission of audit data to an external IT entity as defined in FAU_STG_EXT.1.1 is configurable.

FMT_MOF.1(2)/Audit should only be chosen if the handling of audit data is configurable. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.1.4.

Assurance Activities:

FMT_MOF.1/Audit: The evaluator shall try to modify all parameters for configuration of handling of audit data without prior authentication as administrator. This test should fail.

The evaluator shall try to modify all parameters for configuration of handling of audit data with prior authentication as administrator. This test should pass.

For both kind of tests the evaluator does not necessarily have to test all possible values of all parameters for configuration of handling of audit data but at least one allowed value per configurable parameter.

For the definition of FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions see input for Trusted Update.