Логирование событий JaCarta SecurLogon

Версия ПО: Единый Клиент JaCarta 2.9 и новее

Токены: Любые

Проблема:

Необходимо изучить события, которые связаны с работой JaCarta SecurLogon (например, с целью диагностики сбоя).

Решение:

В журнал событий Windows записываются результаты определенных действий.

Аудит действий пользователя и администратора:

- При выполнении любого из нижеперечисленных действий, должно формироваться сообщение в стандартный журнал событий "Приложение" (Application event log).
- События SecurLogon должны иметь значение атрибута Источник = "JaCarta SecurLogon".
- События, подлежащие аудиту:
    - Вход по профилю SecurLogon (успешный \ неуспешный).
    - Выход (log out) из текущего сеанса ОС.
    - Создание\ удаление\ редактирование профиля SecurLogon.
    - Блокирование рабочей станции: при отключении токена, автоматическая блокировка по истечению заданного времени (стандартная функция ОС) или самостоятельная блокировка пользователем.
    - Автоматическая смена пароля учётной записи.
    - Нарушение целостности продукта (см. требования к надёжности и отказоустойчивости).
- Для каждого события должна быть указана следующая информация:
    - Результат операции – успешный или не успешный.
    - Имя пользователя, инициировавшего изменение, и его SID.
    - Окружение – рабочая станция, домен, рабочая группа.
    - Серийный номер и метка токена.

Дополнительное логирование не ведется.

ID статьи: 226

Последнее обновление: 18 Oct, 2017

Ревизия: 1

JaCarta -> Единый клиент JaCarta -> Логирование событий JaCarta SecurLogon

https://kbp-6.aladdin-rd.ru/index.php?View=entry&EntryID=226