

Cisco ACS 5. X интеграции с символическим сервером SecurID RSA

Содержание

[Введение](#)

[Общие сведения](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Конфигурации](#)

[Сервер RSA](#)

[Версия ACS 5. X-сервер](#)

[Проверка](#)

[Версия ACS 5. X-сервер](#)

[Сервер RSA](#)

[Устранение неполадок](#)

[Создайте запись агента \(sdconf.rec\)](#)

[Перезагрузите \(защищенный\) секретный узел](#)

[Отвергните автоматическое распределение нагрузки](#)

[Вручную вмешайтесь для удаления Выключенного сервера RSA SecurID](#)

Введение

Этот документ описывает, как интегрировать Версию 5.x Системы управления доступом (ACS) Cisco с технологией Проверки подлинности с помощью secureid RSA.

Общие сведения

Cisco Secure ACS поддерживает Сервер RSA SecurID как внешнюю базу данных.

Двухфакторная аутентификация SecurID RSA состоит из персонального идентификационного номера (PIN) пользователя и индивидуально зарегистрированного маркера SecurID RSA, который генерирует коды Token одиночного использования на основе алгоритма временного кода.

Другой код Token генерируется в неподвижных интервалах, обычно каждые 30 или 60 секунд. Сервер RSA SecurID проверяет этот динамический код аутентификации. Каждый маркер SecurID RSA уникален, и не возможно предсказать значение будущего маркера на основе прошлых маркеров.

Таким образом, когда корректный код Token предоставлен вместе с PIN, существует высокая степень уверенности, что человек является допустимым пользователем. Поэтому Серверы RSA SecurID предоставляют механизм более надежной аутентификации, чем обычные повторно используемые пароли.

Можно интегрировать ACS Cisco 5.x с технологией Проверки подлинности с помощью secureid RSA этими способами:

- Агент SecurID RSA - Пользователи аутентифицируются с именем пользователя и кодом доступа через собственный протокол RSA.
- Протокол RADIUS - Пользователи аутентифицируются с именем пользователя и кодом доступа через Протокол RADIUS.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Безопасность RSA
- Система управления доступом Cisco Secure Access Control System (ACS)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Система управления доступом Cisco Secure Access Control System (ACS) версия 5. x
- Символический сервер SecurID RSA

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

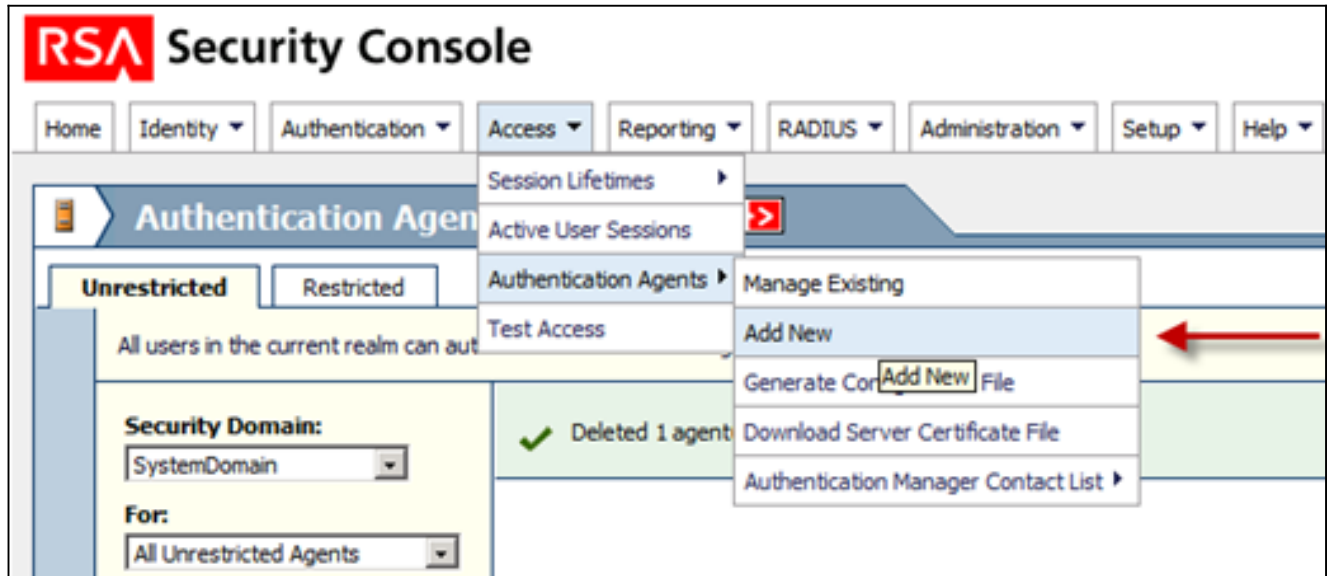
Конфигурации

Сервер RSA

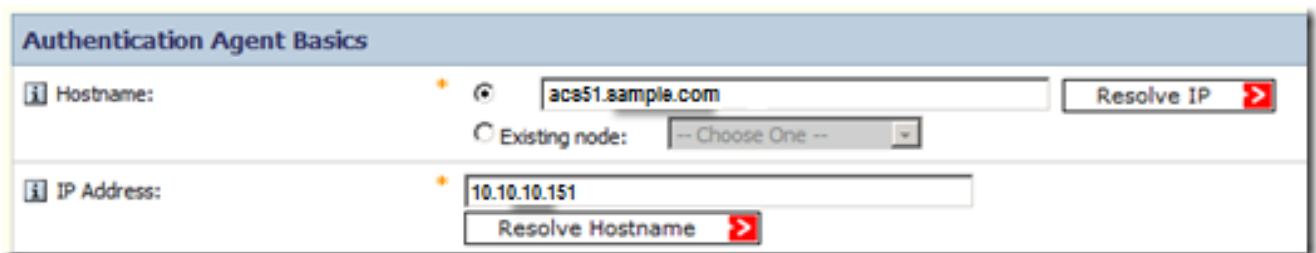
Эта процедура описывает, как администратор Сервера RSA SecurID создает агентов аутентификации и файл конфигурации. Агент аутентификации является в основном названием Сервера доменных имен (DNS) и IP-адресом устройства, программного обеспечения или сервиса, который имеет права обратиться к базе данных RSA. Файл конфигурации в основном описывает топологию RSA и связь.

В данном примере администратор RSA должен создать двух агентов для двух экземпляров ACS.

1. В Консоли Безопасности RSA перейдите для **Доступа>**, **Агенты аутентификации>** добавляют **Новый**:



2. В Add New опознавательном Окне агента определите Имя хоста и IP-адрес для каждого из этих двух агентов:



И DNS вперед и обратные просмотры для агентов ACS должны работать.

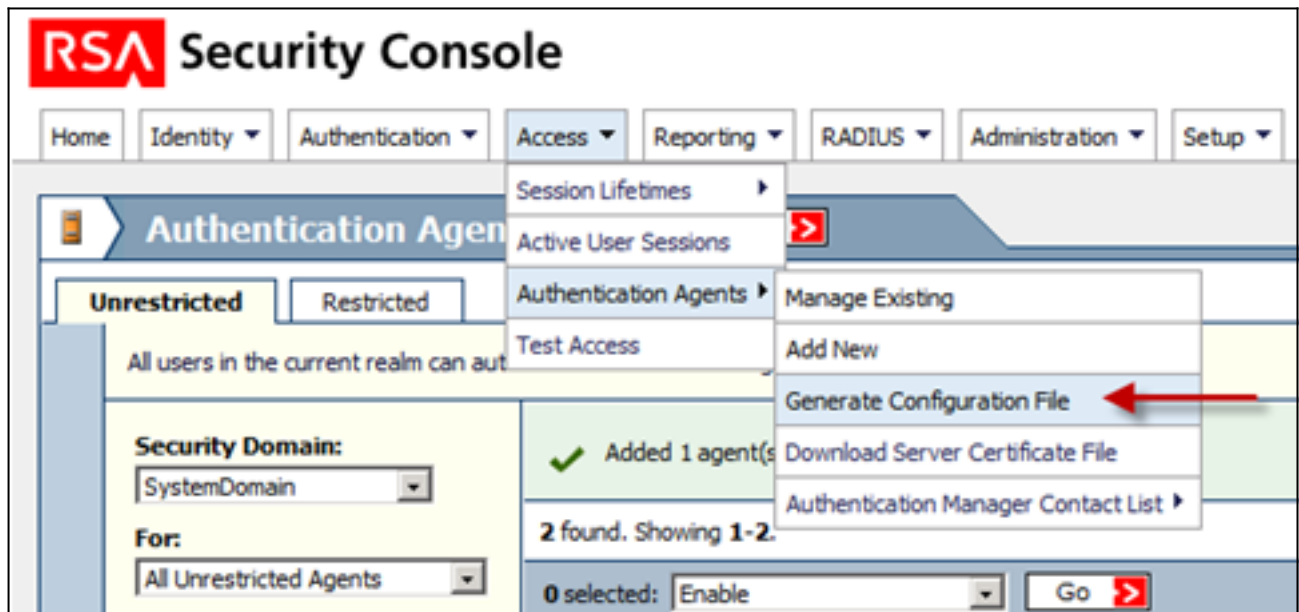
3. Определите тип агента как стандартного агента:



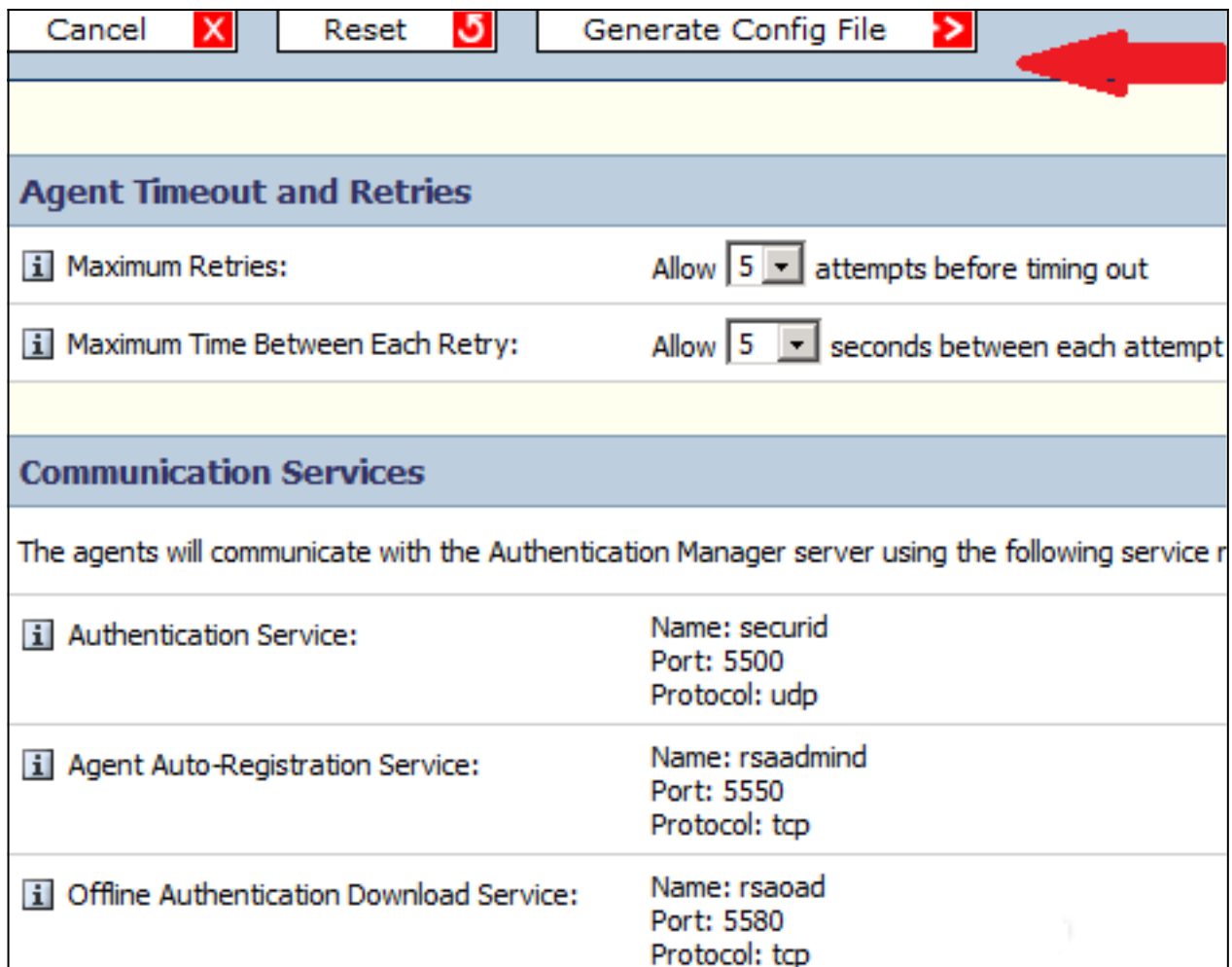
Это - пример информации, которую вы видите, как только добавлены агенты:

| 2 found. Showing 1-2. | | | | | |
|--------------------------|----------------------|--------------|----------------|----------|-----------------|
| 0 selected: Enable [Go] | | | | | |
| <input type="checkbox"/> | Authentication Agent | IP Address | Type | Disabled | Security Domain |
| <input type="checkbox"/> | acs51.sample.com | 10.10.10.151 | Standard Agent | | SystemDomain |
| <input type="checkbox"/> | acs52.sample.com | 10.10.10.152 | Standard Agent | | SystemDomain |
| <input type="checkbox"/> | Authentication Agent | IP Address | Type | Disabled | Security Domain |
| 0 selected: Enable [Go] | | | | | |
| 2 found. Showing 1-2. | | | | | |

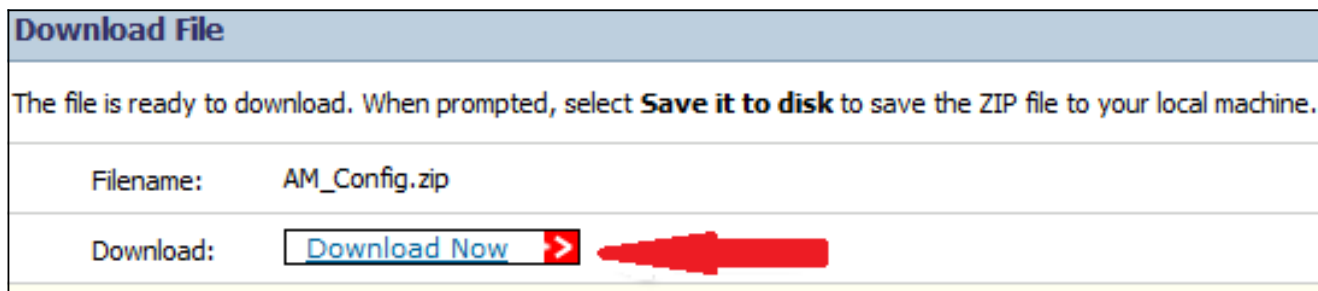
4. В Консоли Безопасности RSA перейдите для **Доступа**, **Агенты аутентификации** > **Генерируют Файл конфигурации** для генерации sdconf.rec файла конфигурации:



5. Используйте значения по умолчанию для Максимальных чисел повторных попыток и Максимальное время Между Каждой Повторной попыткой:



6. Загрузите файл конфигурации:

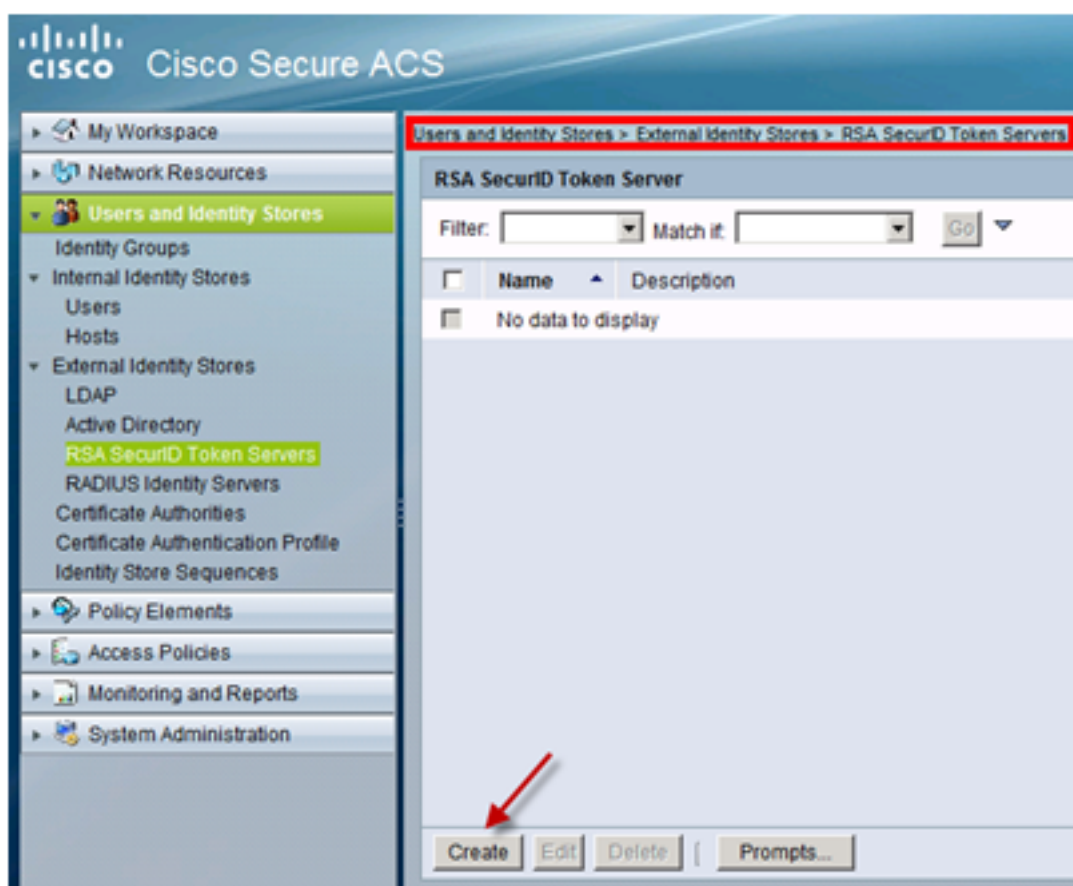


Файл .zip содержит фактическую конфигурацию sdconf.rec файл, в котором администратор ACS нуждается для завершения задач конфигурации.

Версия ACS 5. X-сервер

Эта процедура описывает, как администратор ACS получает и отправляет файл конфигурации.

1. В консоли Версии 5.x Cisco Secure ACS перейдите **Пользователям и Идентификационным Хранилищам > Внешние хранилища идентификаторов > Символические серверы SecurID RSA**, и нажмите **Create**:



2. Введите имя сервера RSA и перейдите к sdconf.rec файлу, который был загружен от сервера RSA:

Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers > Create

RSA Realm ACS Instance Settings Advanced

General

Name: RSA SecurID AM
 Description: RSA SecurID Authentication Manager Server

Server connection

Server Timeout: 30 Seconds
 Reauthenticate on Change PIN

Realm Configuration File

The RSA Configuration file (sdconf.rec) should be provided by your RSA administrator after they have

Import new 'sdconf.rec' file: C:\users\ID\Desktop\sdconf.rec

Node Secret Status: - not created -

* = Required fields

3. Выберите файл и нажмите **Submit**.

Примечание: Первоначально ACS связывается с символическим сервером, другим файлом, названным файлом секретного узла, создан для агента ACS на Менеджере Аутентификации RSA и загружен к ACS. Этот файл используется для зашифрованного подключения.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Версия ACS 5. X-сервер

Для проверки успешной регистрации в системе перейдите к консоли ACS и рассмотрите количество Соответствия:

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals

| | Status | Name | Protocol | Conditions | Results | Hit Count |
|---|--------------------------|------------------------|----------|-------------------------------------------------|-----------------------------|-----------|
| 1 | <input type="checkbox"/> | Rule-4 | -ANY- | NDG:Device Type in All Device Types:SWITCHES | Service RSA Device Admin | 2 |

Можно также рассмотреть Опознавательные Подробные данные от журналов ACS:

| Authentication Details | |
|-----------------------------------------|---------------------------------------------------------------------------------------------------|
| Status: | Passed |
| Failure Reason: | |
| Logged At: | Feb 16, 2013 12:24 PM |
| ACS Time: | Feb 16, 2013 12:24 PM |
| ACS Instance: | <u>acs51</u> |
| Authentication Method: | PAP_ASCII |
| Authentication Type: | ASCII |
| Privilege Level: | 1 |
| User | |
| Username: | TEST1 |
| Remote Address: | |
| Network Device | |
| Network Device: | <u>SwitchBNNZ231</u> |
| Network Device IP Address: | |
| Network Device Groups: | Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN |
| Access Policy | |
| Access Service: | <u>RSA Device Admin</u> |
| Identity Store: | RSA SecurID AM |
| Selected Shell Profile: | PRIVILEGE_15 |
| Active Directory Domain: | |
| Identity Group: | |
| Access Service Selection Matched Rule : | Rule-4 |

Сервер RSA

Для проверки успешной аутентификации перейдите к консоли RSA и рассмотрите журналы:

| Clear Monitor <input type="checkbox"/> | | | | | | | |
|-----------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---------|------------------|----------------|--------------|
| Time | Activity Key | Description | Reason | User ID | Agent | Server Node IP | Client IP |
| i 2013-02-16 12:35:28.764 | Principal authentication | User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain" | <u>Authentication method success</u> | TEST1 | acs51.sample.com | 10.10.10.211 | 10.10.10.151 |

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Создайте запись агента (sdconf.rec)

Для настройки символического сервера SecurID RSA в Версии ACS 5.3 у администратора ACS должен быть sdconf.rec файл. sdconf.rec файл является файлом записи настройки, который задает, как агент RSA связывается с областью Сервера RSA SecurID.

Для создания sdconf.rec файла администратор RSA должен добавить хост ACS как узел агента на Сервере RSA SecurID и генерировать файл конфигурации для этого узла агента.

Перезагрузите (защищенный) секретный узел

После того, как агент первоначально связывается с Сервером RSA SecurID, сервер предоставляет агенту файл секретного узла, названный защищенным. Последующая связь между сервером и агентом полагается на обмен секретным узлом для проверки подлинности других.

Время от времени администраторам, возможно, придется перезагрузить секретный узел:

1. Администратор RSA должен снять флажок с флажком Node Secret Created на записи Узла агента в Сервере RSA SecurID.
2. Администратор ACS должен удалить файл SECURID из ACS.

Отвергните автоматическое распределение нагрузки

Агент SecurID RSA автоматически балансирует запрошенные загрузки на Серверах RSA SecurID в области. Однако у вас есть опция для ручной балансировки загрузки. Можно задать сервер, используемый каждым из узлов агента. Можно назначить приоритет на каждый сервер так, чтобы узел агента направлял запросы аутентификации к некоторым серверам более часто, чем другие.

Необходимо задать настройки приоритета в текстовом файле, сохранить его как sdopts.rec и загрузить его к ACS.

Вручную вмешайтесь для удаления Выключенного сервера RSA SecurID

Когда Сервер RSA SecurID не работает, автоматический механизм исключения не всегда работает быстро. Удалите sdstatus.12 файл из ACS для ускорения этого процесса.