Аутентификация на стороне сервера

Оглавление

1. Введение

Аутентификация на стороне сервера представлена для двух типов:

- **Аутентификация на стороне сервера для менеджеров пользовательского интерфейса**

При использовании серверной аутентификации для менеджеров пользовательского интерфейса пользователь должен пройти аутентификацию в пользовательском интерфейсе через HTTP-сервер. Связь между пользовательским интерфейсом и ядром APDAR (менеджер данных/менеджер событий) возможна только в том случае, если учетные данные для входа проверены HTTP-сервером и обеспечен доступ с помощью токена, специфичного для пользовательского интерфейса.

- **Аутентификация на стороне сервера для менеджеров**

При использовании серверной аутентификации для менеджеров, менеджеры, устанавливающие соединение с менеджером данных или событий, должны пройти аутентификацию. Это повышает безопасность, особенно когда проекты связаны через Интернет. При серверной аутентификации для менеджеров, менеджеры должны аутентифицироваться с помощью сертификатов x.509.

2. Аутентификация на стороне сервера для менеджеров пользовательского интерфейса

- При использовании серверной аутентификации для менеджеров пользовательского интерфейса пользователь должен пройти аутентификацию в пользовательском интерфейсе через HTTP-сервер. Связь между пользовательским интерфейсом и ядром APDAR (менеджер данных/менеджер событий) возможна только в том случае, если учетные данные для входа проверены HTTP-сервером и обеспечен доступ с помощью токена, специфичного для пользовательского интерфейса.

- Аутентификация на стороне сервера для менеджеров пользовательского интерфейса обеспечивает повышенную безопасность, предотвращая несанкционированный доступ клиентов пользовательского интерфейса.

- Аутентификация на стороне сервера для менеджеров пользовательского интерфейса проверяет только самого менеджера. Информацию об аутентификации всех менеджеров см. в главе « Аутентификация на стороне сервера для менеджеров — основы» .

Привязка сессии

- Привязка сессии снижает риск манипулирования сообщениями и несанкционированного доступа к системе APDAR. Повышается безопасность связи, поскольку предотвращается доступ неавторизованных администраторов. При привязке сессии имя пользователя APDAR является частью сертификата. Инструкции по созданию сертификата с именем пользователя см. в главе **«Панель для SSL-сертификатов»** .

- Привязка сессии активируется через серверную аутентификацию для менеджеров пользовательского интерфейса. При загрузке плагина контроля доступа привязка сессии автоматически активируется и не может быть деактивирована. По умолчанию (стандартный проект) привязка сессии деактивирована. Вы можете активировать ее независимо от плагина контроля доступа, используя параметр конфигурации serverSideAuthentication=1 в разделе [general].

2.1. Требования и установка

Для успешной настройки серверной аутентификации для менеджеров пользовательского интерфейса необходимо выполнить следующие шаги.

Конфигурация на стороне сервера

1. Активация автоматической разблокировки в управлении устройством.
2. Описание используемого плагина контроля доступа
3. Определение веб-сервера

Конфигурация на стороне клиента

1. Выполнение конфигурации, специфичной для клиента, например, удаленного пользовательского интерфейса или ULC UX.
2. Выполните дополнительные необязательные настройки .
3. Запуск серверного проекта, опция -ssa и файл webclient_http.ctl.

Внимание:

Для аутентификации на стороне сервера (SSA) в мобильных пользовательских интерфейсах необходимо использовать плагины APDAR AccessControlPlugin и AccessControlPluginUser. Использование плагинов, специфичных для пользователя, не допускается. Аутентификация на стороне сервера (SSA) может использоваться с мобильным пользовательским интерфейсом. Использование SSA на мобильных устройствах противоречит предполагаемому назначению функций мобильного пользовательского интерфейса и SSA. Даже если SSA применяется к мобильным пользовательским интерфейсам в проекте, мобильные устройства/мобильный пользовательский интерфейс нельзя считать безопасными.

Обратите внимание, что проект для серверной аутентификации для менеджеров пользовательского интерфейса также можно создать через панель администрирования проектов — см. главу « Создание проекта» .

Конфигурация на стороне сервера

Примечание:

В проекте SSA для входа в систему нельзя использовать пользователя root . Однако вы можете использовать всех остальных пользователей, например, пользователя "para". Предопределенных пользователей, создаваемых по умолчанию при создании проекта, можно найти в главе " Пользователи ". Чтобы создать новых пользователей, см. главу " Пользователи " . Инструкции по настройке прав доступа пользователей см. в главе " Группы" .

При использовании единого входа (Single Sign On) аутентификация на стороне сервера для менеджеров пользовательского интерфейса не поддерживается.

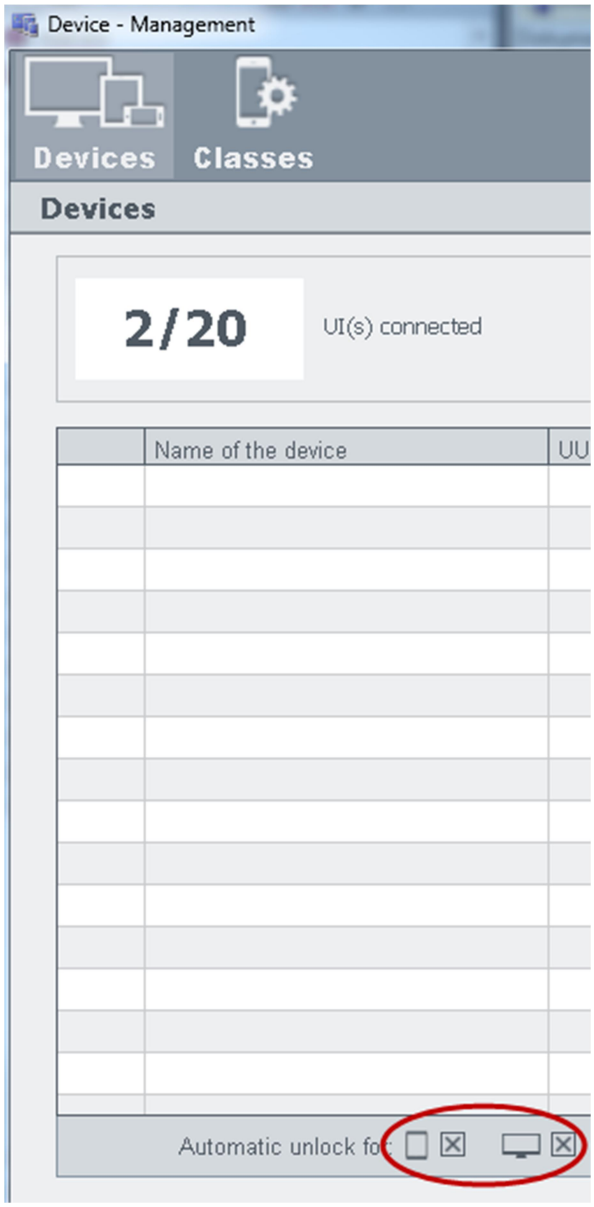
После добавления записей конфигурации и менеджера CTRL запустите свой проект. Если проект уже запущен, потребуется его перезапуск.

Управление устройствами - автоматическая разблокировка

Перед установкой параметра конфигурации "AccessControlPluginUser" включите автоматическую разблокировку в панели управления устройством (Панель управления системой -> Настройки -> Устройство - Управление) (см. рисунок ниже).

После включения серверной аутентификации для активации менеджеров пользовательского интерфейса запустите пользовательский интерфейс. Затем снова отключите автоматическую разблокировку в управлении устройством.

Рисунок: Управление устройствами



Настройка - Плагин контроля доступа

Для успешной настройки серверной аутентификации для менеджеров пользовательского интерфейса в конфигурационном файле необходимо указать следующие 2 параметра.

[general]

accessControlPlugin = "AccessControlPluginUser"

Примечание:

При использовании серверной аутентификации для менеджеров используйте соответствующую запись в конфигурации.

[general]

accessControlPlugin = "AccessControlPlugin"

Параметр " accessControlPlugin " определяет, какой плагин используется для аутентификации на стороне сервера для менеджеров пользовательского интерфейса или для аутентификации на стороне сервера для менеджеров. См. также раздел "Интерфейс контроля доступа, основы".

[webClient]

clientSideAuth = 0

Параметр clientSideAuth = 0 указывает на использование серверной аутентификации для менеджеров пользовательского интерфейса.

Конфигурация - Веб-сервер

Укажите веб-сервер следующим образом:

[ui]

httpServer = "https://localhost:443"

Примечание:

Если SSA тем временем деактивирована, удалите соответствующее значение параметра _UIx.SessionToken от имени пользователя root. В противном случае панель входа в систему будет отображаться некорректно для ранее открытого пользовательского интерфейса, и у пользователя, автоматически вошедшего в систему, не будет пользовательских прав.

Конфигурация на стороне клиента

Для соответствующих используемых клиентов требуется следующая настройка:

Удалённая настройка пользовательского интерфейса / пользовательского интерфейса рабочего стола

При использовании удалённого пользовательского интерфейса или интерфейса рабочего стола в конфигурационный файл вашего серверного проекта необходимо добавить следующие записи:

[general]

accessControlPlugin = "AccessControlPluginUser"

При использовании серверной аутентификации для менеджеров используйте соответствующую запись в конфигурации.

[general]

accessControlPlugin = "AccessControlPlugin"

Для использования аутентификации по HTTP-серверу добавьте в раздел webClient файла конфигурации запись httpAuth = 1, а также записи httpsPort и httpPort.

[webClient]

httpAuth=1

httpsPort = 443

httpPort = 0

Конфигурация пользовательского интерфейса ULC

Для активации серверной аутентификации ULC UX добавьте следующие записи в конфигурационный файл вашего серверного проекта:

[httpServer]

uiArguments = "-p vision/login.pnl -centered -iconBar -menuBar -ssa"

Дополнительная конфигурация

aliveTimeout

В случае высокой задержки сетевого соединения между клиентом и сервером может потребоваться увеличить значение aliveTimeout для обмена данными и событиями через менеджер, например:

[данные]

aliveTimeout = -2

[событие]

aliveTimeout = -2

uiUsesMainServerAsFileServer

Параметр "uiUsesMainServerAsFileServer =0" необходим для предотвращения перенаправления пользовательского интерфейса на дополнительный веб-сервер для загрузки файлов проекта. В этом случае все файлы (панели, скрипты и т. д.), необходимые для пользовательского интерфейса, должны находиться внутри проекта, используемого для запуска сервера ULC UX.

[httpServer]

uiUsesMainServerAsFileServer = 0

Стартовая панель

Чтобы указать стартовую панель при запуске пользовательского интерфейса, используйте либо запись rootPanel для UI:

[webClient]

rootPanel = "vision/login.pnl"

или запись mobileRootPanel для мобильного пользовательского интерфейса приложения :

[webClient]

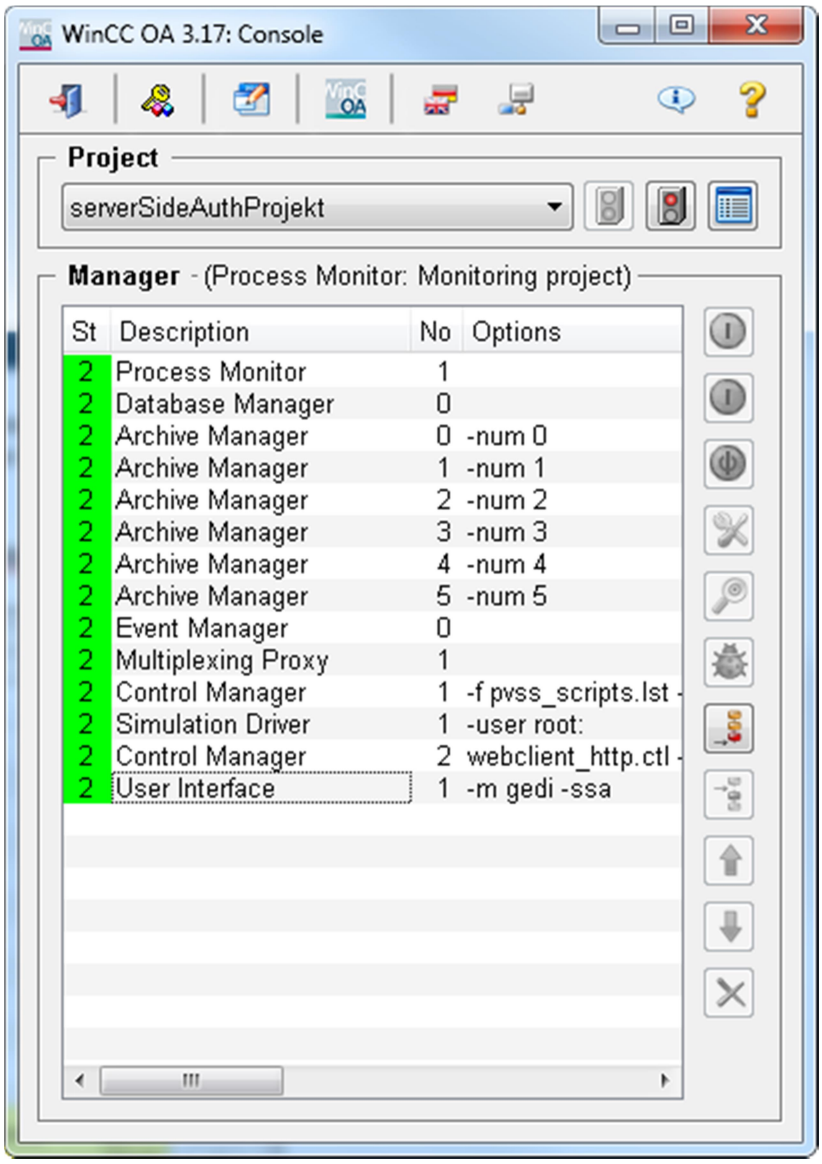
mobileRootPanel = "vision/login.pnl"

Если эти параметры конфигурации не заданы, отображается файл login.pnl.

Запуск серверного проекта

Запустите проект сервера. Добавьте опцию -ssa, чтобы клиент мог подключиться к HTTP-серверу APDAR, и добавьте скрипт webclient_http.ctl в проект. См. рисунок ниже (здесь в качестве сервера используется локальный компьютер localhost):

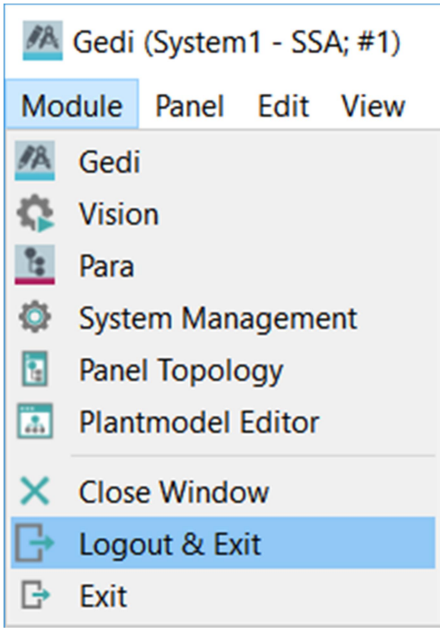
Рисунок: Проект сервера и опция -ssa, а также скрипт webclient_http.ctl



Теперь вы можете запустить любой клиент по вашему выбору, например ULC UX, по адресу *https://localhost/data/ulc/start.html*

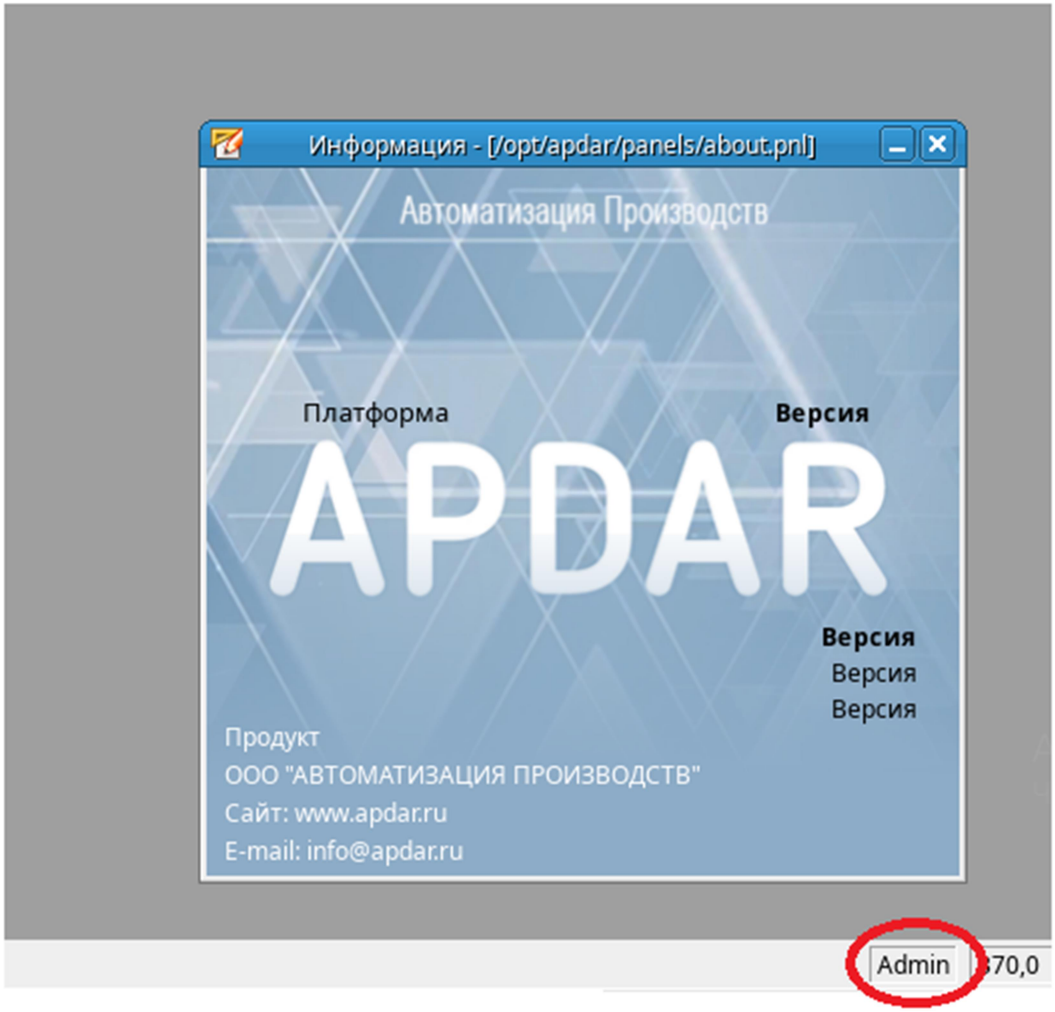
- В каждом модуле есть опция "Выход и завершение работы", если пользовательский интерфейс был запущен с опцией -ssa. Опция "Выход и завершение работы" удаляет из списка сохраненных учетных данных имя пользователя/пароль, сохраненные с помощью флажка в диалоговом окне аутентификации. Таким образом, при следующем запуске пользовательского интерфейса отображается диалоговое окно HTTP-аутентификации.

Рисунок: Опция «Выход из системы»



В строке состояния GEDI теперь появилось дополнительное поле, отображающее имя текущего пользователя:

Рисунок: Имя пользователя в строке состояния



Обратите внимание, что имя пользователя заполняется только при запуске. Если во время работы GEDI произойдет изменение пользователя, поле не будет обновлено.

2.2. Примечания и ограничения

При использовании серверной аутентификации для менеджеров пользовательского интерфейса необходимо учитывать следующие замечания и ограничения:

-ssa Параметр менеджера пользовательского интерфейса

Новый параметр менеджера пользовательского интерфейса «-ssa» определяет, что при одновременном использовании параметра «-server» загрузка файлов проекта и связанное с этим создание кэша проекта не выполняются. Этот параметр следует использовать, если все файлы, необходимые для работы пользовательского интерфейса, уже находятся на клиентском компьютере, используемом для запуска пользовательского интерфейса.

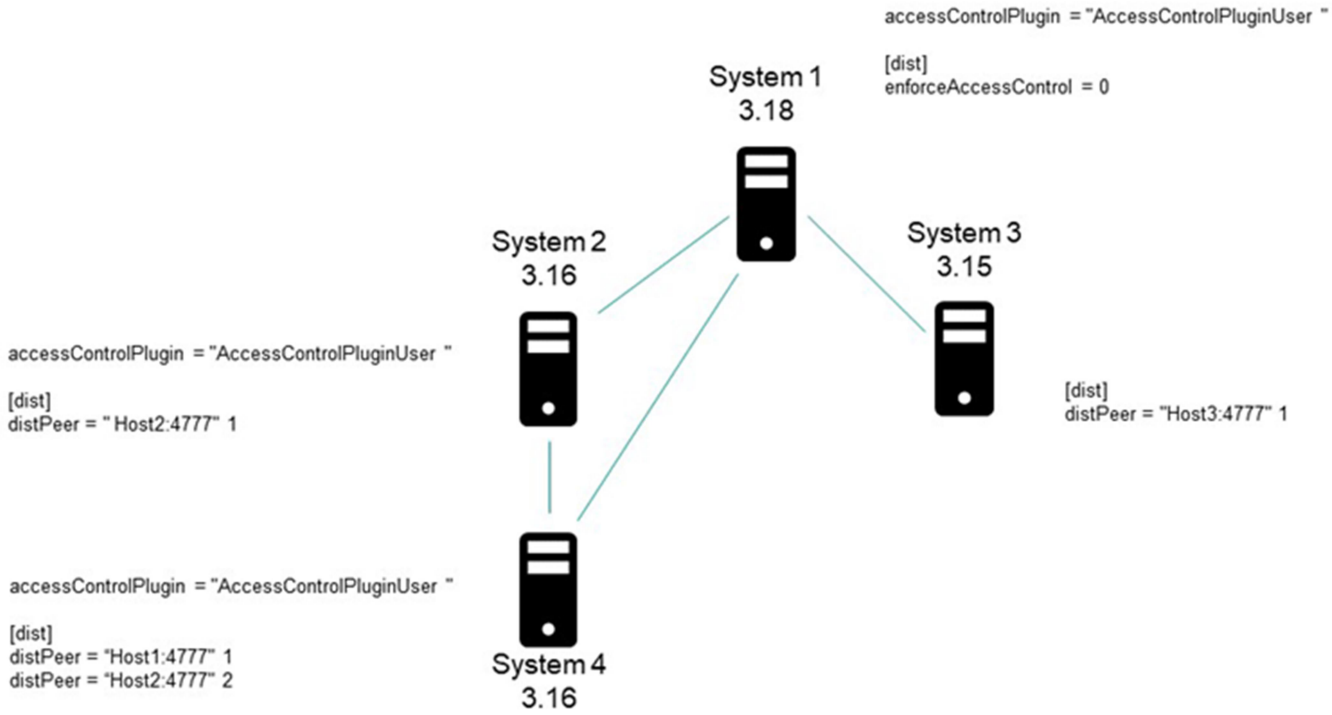
Аспект безопасности

Обратите внимание, что использование серверной аутентификации для менеджеров пользовательского интерфейса само по себе не повысит безопасность вашего предприятия. Для обеспечения надлежащей защиты объекта необходимо соблюдать требования, описанные в Руководстве по безопасности .

Аутентификация пользовательского интерфейса

Аутентификация на стороне сервера для менеджеров пользовательского интерфейса выполняет только аутентификацию самого менеджера. Аутентификация других менеджеров, например dist, redu или ctrl, не выполняется. Однако плагин загружается всеми менеджерами и, следовательно, необходим для всего взаимодействия между ними.

Рисунок DIST Проекты SSA и более старые проекты, не относящиеся к SSA



Если вы не можете обновить старую систему APDAR , которая еще не поддерживает аутентификацию на стороне сервера (<=3.15), вы можете отключить аутентификацию на стороне сервера для этого соединения DIST с помощью параметра конфигурации enforceAccessControl=0 (в разделе dist файла конфигурации). Отключение допускается только в том случае, если оценка рисков показывает, что это неактуально, например, в доверенной зоне. Мы рекомендуем использовать последние обновления для всех систем APDAR . На рисунке ниже показана возможная конфигурация DIST с различными версиями APDAR .

Ограничения

Необходимо учитывать следующие ограничения:

- Для смены пользователя в пользовательском интерфейсе ULC требуется перезапуск браузера. В противном случае смена пользователя невозможна.
- При использовании единого входа (Single-Sign-On) аутентификация на стороне сервера для менеджеров пользовательского интерфейса не поддерживается.

3. Аутентификация на стороне сервера для менеджеров

При использовании серверной аутентификации для менеджеров, менеджеры, устанавливающие соединение с менеджером данных или событий, должны пройти аутентификацию. Это повышает безопасность, особенно когда проекты связаны через Интернет. При серверной аутентификации для менеджеров, менеджеры должны аутентифицироваться с помощью сертификатов x.509.

По этой причине вам нужны сертификаты. Вы можете создать свои сертификаты самостоятельно. Для создания сертификатов используйте панель SSL-сертификатов. Вы можете открыть панель через вкладку «Управление системой» -> «Связь». Как создавать сертификаты с помощью файлов цепочек, описано в руководстве по безопасности . С помощью файлов цепочек вы можете создать несколько цепочек, и аутентификация может использоваться, например, в нескольких частях предприятия. Файлы цепочек можно использовать для разных частей предприятия. Инструкции по использованию файла цепочки см. в разделе «Пример конфигурации» . Вы также можете использовать сертификаты хранилища сертификатов Windows .

В резервированной системе и в системе DRS плагин контроля доступа должен быть настроен для обеих систем. Другими словами, настройки в обеих системах должны быть одинаковыми.

Аутентификация на стороне сервера для менеджеров используется для всех менеджеров. Информацию об аутентификации менеджеров пользовательского интерфейса см. в главе « Основы аутентификации на стороне сервера для менеджеров пользовательского интерфейса» .

Привязка сессии

Привязка сессии снижает риск манипулирования сообщениями и несанкционированного доступа к системе APDAR . Повышается безопасность связи, поскольку предотвращается доступ неавторизованных администраторов. При привязке сессии имя пользователя APDAR является частью сертификата; см. главу «Панель для SSL-сертификатов» о том, как создать сертификат с именем пользователя.

Привязка сессии активируется через серверную аутентификацию для менеджеров пользовательского интерфейса . При загрузке плагина контроля доступа ETM привязка сессии автоматически активируется и не может быть деактивирована. По умолчанию (стандартный проект) привязка сессии деактивирована. Вы можете активировать ее независимо от плагина контроля доступа, используя параметр конфигурации serverSideAuthentication=1 в разделе [general].

3.1. Требования и установка

Для успешной настройки серверной аутентификации для менеджеров необходимо выполнить следующие шаги.

Конфигурация на стороне сервера

Следующие шаги уже были описаны в документации по серверной аутентификации для менеджеров пользовательского интерфейса. Подробности см. в главе « Требования и установка» .

1. Активация автоматической разблокировки в управлении устройством.
2. Описание используемого плагина контроля доступа
3. Запуск скрипта webclient_http.ctl с использованием нового или существующего менеджера команд CTRL.
4. Выполнение конфигурации, специфичной для клиента, например, удаленного пользовательского интерфейса или ULC UX.
5. Запуск серверного проекта
6. Запуск клиента

Помимо вышеперечисленных требований, должны быть выполнены следующие условия:

Необходимо создать сертификаты. Обратите внимание, что для каждого пользователя, от имени которого вы хотите запустить менеджер, необходимо сгенерировать отдельный сертификат. Для аутентификации можно использовать всех пользователей. См. главу « Панель для SSL-сертификатов хоста» или используйте сертификат из хранилища сертификатов Windows .

В проекте SSA (UI) для входа в систему нельзя использовать пользователя root . Однако можно использовать всех остальных пользователей, например, пользователя «para». Предопределенных пользователей, создаваемых по умолчанию при создании проекта, можно найти в главе « Пользователи ». Чтобы создать новых пользователей, см. также главу « Пользователи » . Инструкции по настройке прав доступа пользователей см. в главе « Группы» .

Обратите внимание, что проект для серверной аутентификации менеджеров также можно создать через панель администрирования проектов — см. главу « Создание проекта» .

Для целей аутентификации сертификаты должны содержать совпадающее имя пользователя. Сертификаты по умолчанию, поставляемые с установкой APDAR, обеспечивают только безопасность соединения и не содержат никакой информации о пользователе. Создайте сертификаты, содержащие имя пользователя, либо через панель управления SSL-сертификатами хоста с помощью файла openssl.cnf, либо через командную строку — см. Руководство по безопасности .

Задайте параметры конфигурации ssaChainFile , ssaCertificate и ssaPrivateKey в разделе [general] или в разделе, специфичном для менеджера, файла конфигурации. Если вы используете список отзыва сертификатов, задайте также параметр ssaCRL в разделе [general] или в разделе, специфичном для менеджера, файла конфигурации. Пример параметров конфигурации см. в главе « Параметры конфигурации для SSA для менеджеров» , а полный пример — в главе « Пример конфигурации — SSA для менеджеров» . Если вы используете сертификаты хранилища сертификатов Windows ,

вам также потребуется параметр конфигурации ssaCertCheck , но не параметр конфигурации ssaChainFile.

ВНИМАНИЕ:

Все менеджеры, не использующие пользователя "root", должны использовать параметр менеджера -user username. Этот параметр работает без необходимости ввода пароля. Пример см. в главе " Пример конфигурации - Конфигурация SSA - SSA для менеджеров" .

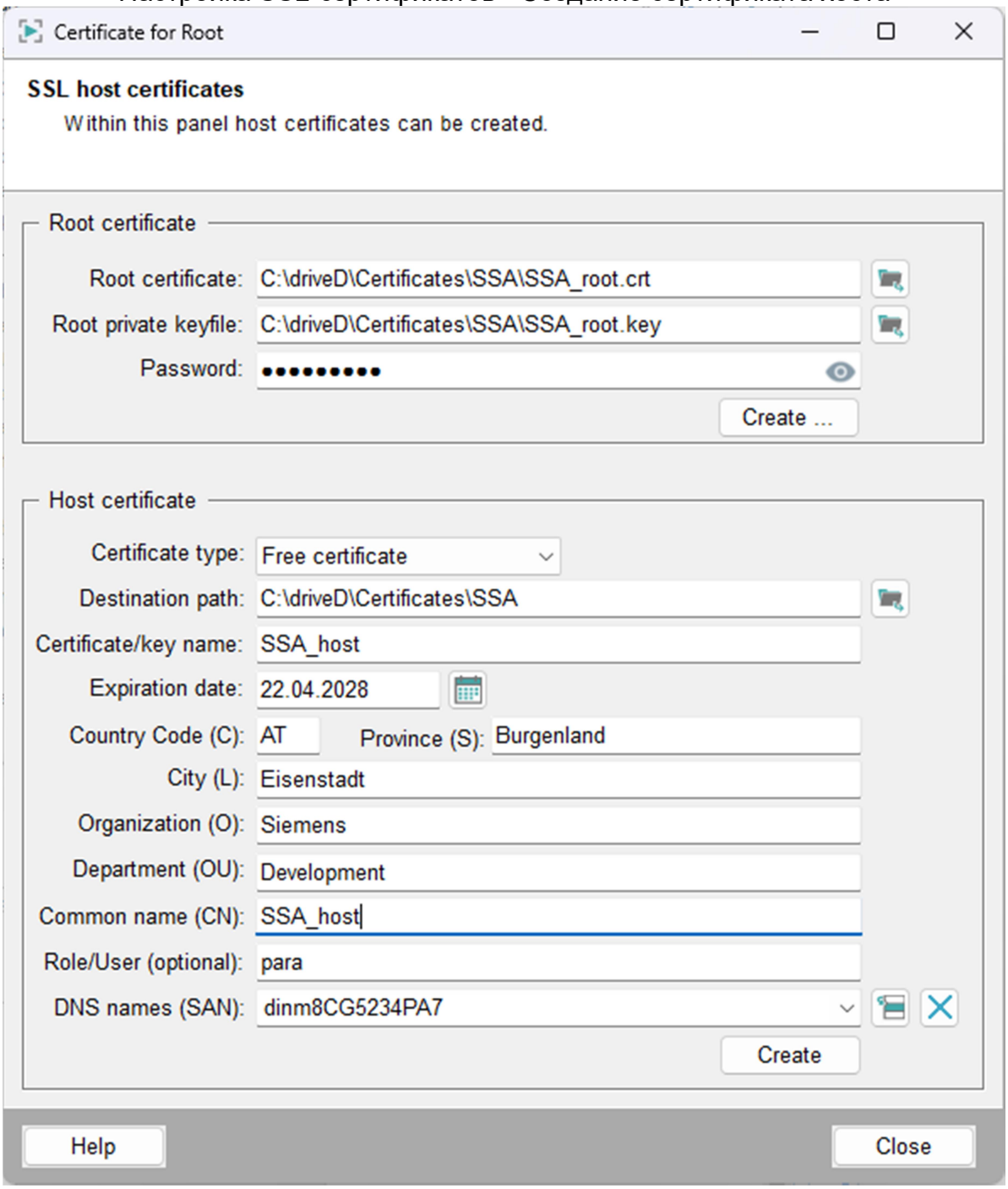
Флаг отладки

Для аутентификации доступен флаг отладки -dbg SSA.

3.2. Панель для SSL-сертификатов хоста

Откройте панель SSL-сертификатов через «Управление системой» > «Связь» > «SSL-сертификаты».

Настройка SSL-сертификатов - Создание сертификата хоста



Эта панель позволяет создавать новые сертификаты для ваших хостов. При использовании имен сертификатов по умолчанию, например, host-cert.pem, и автоматической генерации сертификатов, они также автоматически копируются на хост. Если вы создаете сертификаты самостоятельно, их необходимо скопировать на соответствующие хосты для дальнейшего использования.

APDAR позволяет создавать сертификаты, которые можно использовать для

- Аутентификация менеджеров на стороне сервера .
- Мультиплексный прокси
- HTTP-сервер
- WebView.ewo

- Руководитель отдела отчетности
- ОПК UA
- Мобильное приложение с пользовательским интерфейсом и
- Пользовательский интерфейс для настольных компьютеров

Панель разделена на следующие секции:

- Корневой сертификат
- Сертификат хоста

3.3. Пример конфигурации - SSA для менеджеров

1. Создайте проект или используйте существующий.
2. Используйте как центр сертификации, так и созданные вами доступные сертификаты.

ВНИМАНИЕ:

Сертификаты должны располагаться на том же разделе, что и проект APDAR . Если проект, например, сохранен на диске D:, то и сертификаты должны быть сохранены на диске D:.

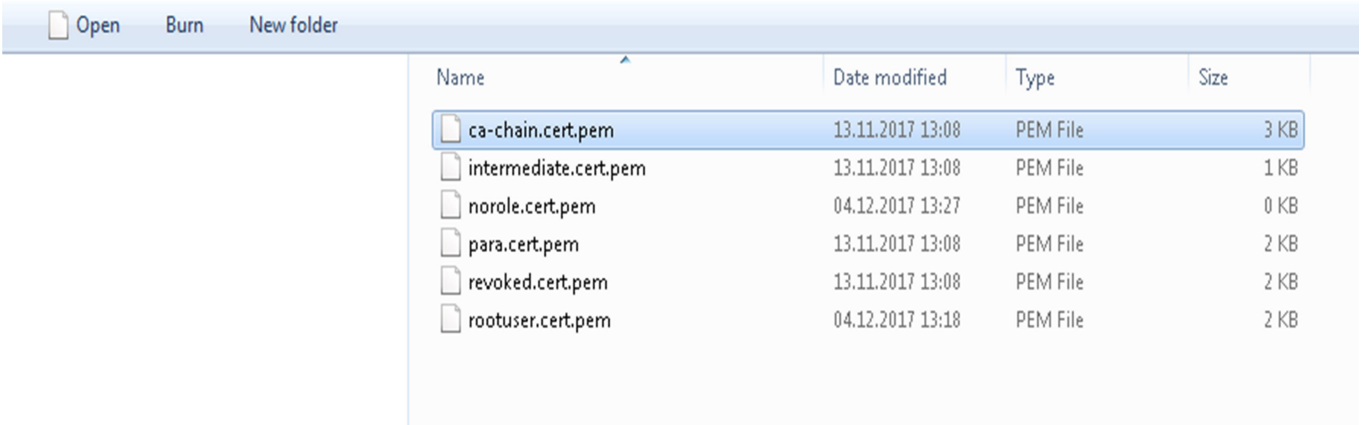
ВНИМАНИЕ:

Сертификаты не должны сохраняться в проекте по соображениям безопасности. Исключением являются сертификаты веб-сервера . Они автоматически копируются в проект. Сертификаты веб-сервера используются для всех функций, требующих работы веб-сервера. К таким функциям относятся, например, пользовательский интерфейс для настольных компьютеров и пользовательский интерфейс ULC .

3. Вам потребуются следующие сертификаты:

- ca-chain.cert.pem. Файл ca-chain.cert.pem необходим только для сервера. Он служит для проверки сертификатов.

Рисунок файла ca-chain.cert.pem



- Используйте файлы сертификатов norole.cert.pem, para.cert.pem, revoked.cert.pem, а также rootuser.cert.pem и crl.cert.pem.

На рисунке показаны файлы norole.cert.pem, para.cert.pem, revoked.cert.pem, а также rootuser.cert.pem.

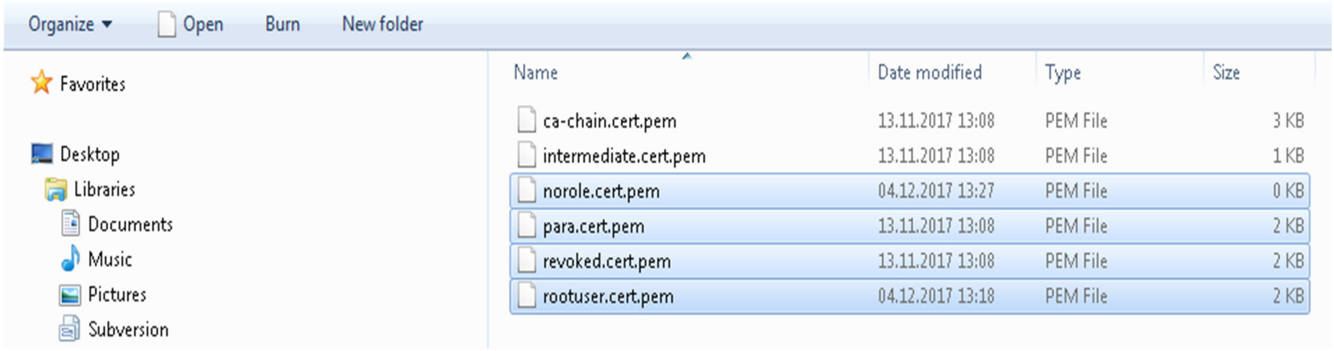
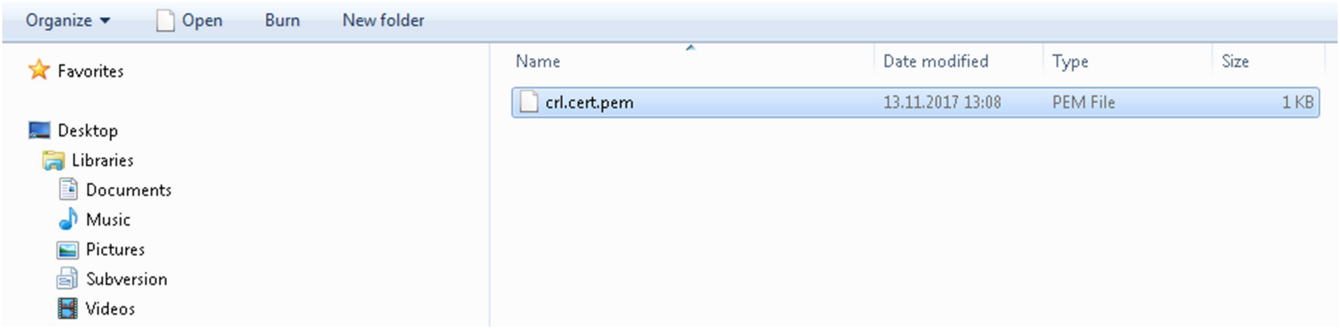


Рисунок файла crl.cert.pem

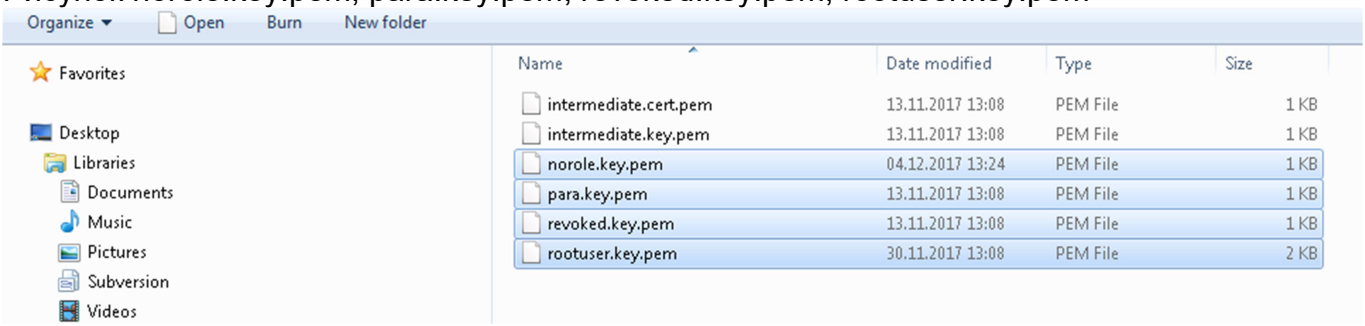


- Вам также понадобятся ключи:
    - norole.key.pem
    - para.key.pem
    - revoked.key.pem
    - rootuser.key.pem

Примечание:

Ключи должны существовать только на компьютере, где менеджер использует их для аутентификации. На сервере (если сервер запускает своих менеджеров только от имени пользователя root) требуется только один файл rootuser.key.pem. Остальные ключи необходимы только на клиентах, подключающихся к серверу. Для аутентификации этих клиентов серверу нужен только файл цепочки ключей.

Рисунок norole.key.pem, para.key.pem, revoked.key.pem, rootuser.key.pem



4. Укажите следующие параметры конфигурации:

[general]

accessControlPlugin = "AccessControlPlugin"

[webClient]

clientSideAuth = 0

httpsPort = "443"

httpPort = "0"

rootPanel = "vision/login.pnl"

mobileRootPanel = "vision/login.pnl"

[ui]

httpServer = "https://localhost:443"

ВНИМАНИЕ:

При использовании серверной аутентификации для UI Managers используйте параметр конфигурации [general] accessControlPlugin = "AccessControlPluginUser"

Следующие настройки сервера:

[general]

ssaChainFile = "SSA_cert/ca-chain.cert.pem"

ssaCRL = "SSA_cert/crl.cert.pem"

Примечание:

В этом примере используется файл цепочки сертификатов (см. выше). Если вы используете сертификаты из хранилища сертификатов Windows , вам потребуется запись конфигурации "ssaChertCheck".

Для всех диспетчеров управления установлены следующие параметры:

[general]

ssaPrivateKey = "file:SSA_cert/rootuser.key.pem"

ssaCertificate = "file:SSA_cert/rootuser.cert.pem"

The following settings for the UI manager:
[httpServer]
uiArguments = "-p vision/login.pnl -centered -iconBar -menuBar -ssa"

The following settings for different Control managers:
[ctrl_3]
ssaPrivateKey = "file:SSA_cert/para.key.pem"
ssaCertificate = "file:SSA_cert/para.cert.pem"

[ctrl_4]
ssaPrivateKey = "file:SSA_cert/revoked.key.pem"
ssaCertificate = "file:SSA_cert/revoked.cert.pem"

[ctrl_5]
ssaPrivateKey = "file:SSA_cert/norole.key.pem"
ssaCertificate = "file:SSA_cert/norole.cert.pem"

[ctrl_6]
ssaPrivateKey = "file:SSA_cert/para.key.pem"
ssaCertificate = "file:SSA_cert/para.cert.pem"

Рисунок. Файл конфигурации с записями конфигурации.

5. Создайте в редакторе скриптов 3 скрипта, содержащих, например, следующий код:

```
void main()
{
  DebugTN("The script 1 is running");
}
```

6. В консоли добавьте 5 менеджеров CTRL и один менеджер пользовательского интерфейса со следующими параметрами:

CTRL -num 2 webclient_http.ctl

UI -m gedi -ssa

CTRL -num 3 script1.ctl -user para:

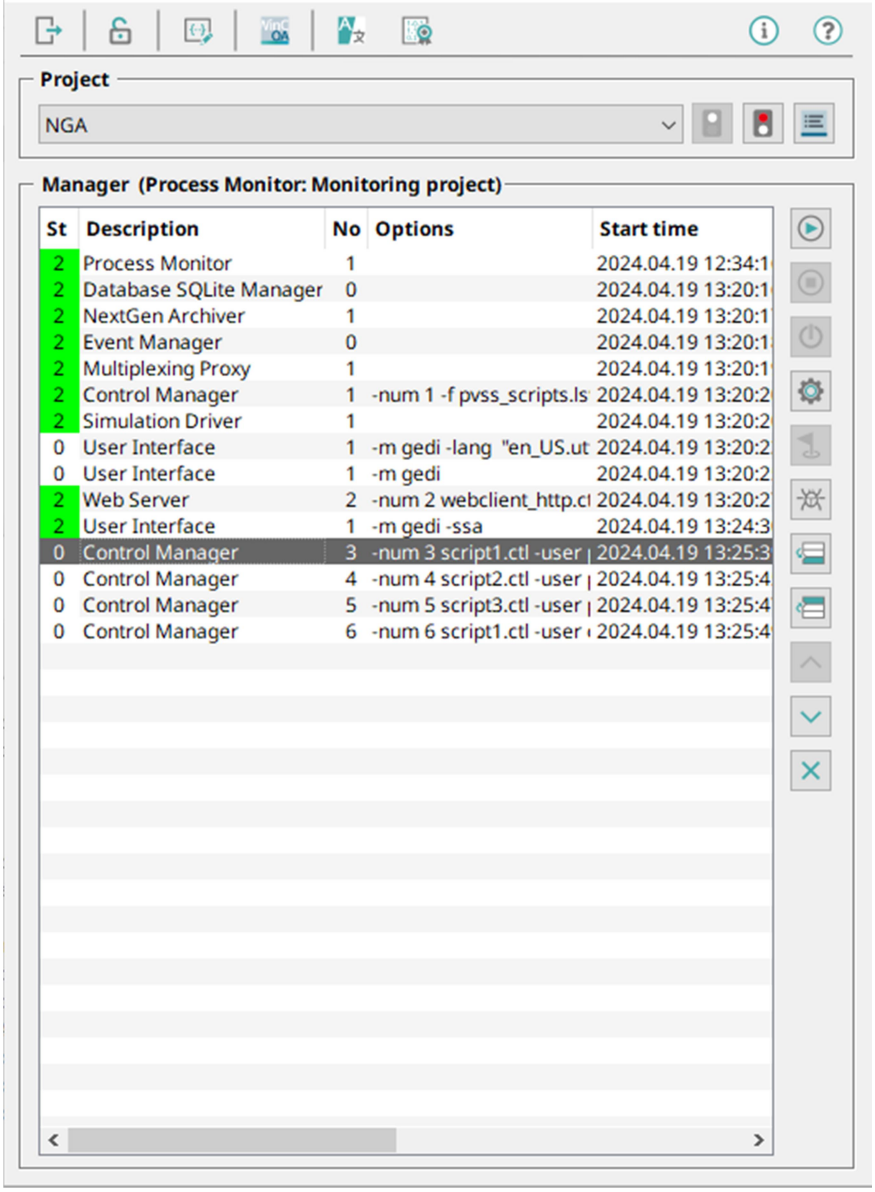
CTRL -num 4 script2.ctl -user para: //The option does not work since the wrong certificate is available, no //certificate for the user para but for the user "revoked"

CTRL -num 5 script3.ctl -user para: //The option does not work since the wrong certificate is available, no //certificate for the user para, but for the user "norole".

CTRL -num 6 script1.ctl -user operator: //The option does not work since this is the wrong user

//not the user para but the user "operator"

Отображение консоли с запущенными менеджерами



If you start the script 1, the following is output in the log viewer:

WCCOActrl (3), 2017.12.04 15:36:41.746, SYS, INFO, 103, User names/passwords initialized

WCCOActrl3:2017.12.04 15:36:41.878["The script 1 is running"]

WCCOActrl (3), 2017.12.04 15:36:43.879, SYS, INFO, 181, Closing connection to (SYS: 0 Data -num 0 CONN: 1)

3.4. Настройки SSA для менеджеров

В серверной аутентификации (SSA) для менеджеров менеджеры должны проходить аутентификацию с помощью сертификатов. В этой главе приведены параметры конфигурации, необходимые для использования сертификатов в проекте APDAR SSA для менеджеров.

ВНИМАНИЕ:

Обратите внимание, что перед установкой параметров конфигурации вам необходимо создать собственные сертификаты и настроить аутентификацию на стороне сервера для менеджеров .

SSL-связь с использованием файловых сертификатов

Запись конфигурации	Описание
[general] accessControlPlugin ="AccessControlPlugin"	**Аутентификация на стороне сервера для менеджеров:** [general] accessControlPlugin = "AccessControlPlugin" Загружает плагин accessControlPlugin и активирует серверную аутентификацию для менеджеров (см. раздел «Серверная аутентификация для менеджеров: основы »). **Аутентификация на стороне сервера для менеджеров пользовательского интерфейса:** При использовании серверной аутентификации для менеджеров пользовательского интерфейса используйте следующую запись в конфигурации. [general] accessControlPlugin = "AccessControlPluginUser" Это активирует аутентификацию на стороне сервера для менеджеров пользовательского интерфейса.
[webClient] clientSideAuth = 0 httpsPort = 443 httpPort = 0 rootPanel = "vision/login.pnl" mobileRootPanel = "vision/login.pnl"	Параметр clientSideAuth активирует аутентификацию на стороне сервера . Кроме того, вам потребуется параметр конфигурации "accessControlPlugin", см. выше. С помощью параметра httpsPort вы указываете порт по умолчанию для HTTPS-соединения, а с помощью параметра httpPort устанавливаете HTTP-порт на 0. Параметр httpPort отключен. Чтобы указать стартовую панель при запуске пользовательского интерфейса, используйте либо

	запись rootPanel для UI: [webClient] rootPanel = "vision/login.pnl" или запись mobileRootPanel для мобильного пользовательского интерфейса приложения : [webClient] mobileRootPanel = "vision/login.pnl" Если эти параметры конфигурации не заданы, отображается login.pnl, поскольку это панель по умолчанию. Вы можете указать свою собственную панель, в противном случае будет отображаться панель по умолчанию.
[ui] httpServer = "https://localhost:443"	Укажите веб-сервер и номер порта.
КОРНЕВОЙ СЕРТИФИКАТ: [general] ssaChainFile = "root-cert.pem" **КЛЮЧ ХОСТА И СЕРТИФИКАТ ХОСТА:** [general] ssaPrivateKey = "file:hostUserName.key" ssaCertificate = "file:hostUserName.crt" Также можно использовать сертификаты и ключи с расширением .pem: ssaCertificate = "file:hostUserName.cert.pem" ssaPrivateKey = "file:hostUserName.key.pem"	КОРНЕВЫЙ СЕРТИФИКАТ: • Параметр ssaChainFile указывает путь к файлу корневого сертификата. Если вы создадите стандартный проект по умолчанию , сертификат в файле ssaChainFile будет называться "root-cert.pem". • Если в разделе [general] конфигурационного файла задан параметр "ssaChainFile", все менеджеры должны использовать файловые сертификаты. Если этот параметр задан, AccessControlPlugin не проверяет сертификаты в хранилище сертификатов Windows. **Примечание:** Также поддерживаются промежуточные сертификаты. См. рекомендации по безопасности APDAR . КЛЮЧ ХОСТА И СЕРТИФИКАТ ХОСТА: • Параметры ssaPrivateKey и ssaCertificate указывают файл ключа хоста и сертификат хоста: ssaPrivateKey = "file:hostUserName.key" ssaCertificate = "file:hostUserName.crt" файл: префикс указывает, что ключ и сертификат загружаются из файла.
[httpServer] uiArguments = "-p vision/login.pnl -centered -iconBar -menuBar -ssa"	Для активации серверной аутентификации пользовательского интерфейса ULC добавьте параметр конфигурации uiArguments в файл конфигурации вашего серверного проекта.

Пример серверной аутентификации для менеджеров см. в главе « Пример конфигурации — SSA для менеджеров» .

SSL-связь с сертификатами хранилища сертификатов Windows:

Запись конфигурации	Описание
[general] accessControlPlugin = "AccessControlPlugin" ssaCertCheck ="chainPrefix=root_SSA"	Загружает accessControlPlugin . См. раздел «Серверная аутентификация для менеджеров пользовательского интерфейса: основы ». При использовании серверной аутентификации для менеджеров пользовательского интерфейса используйте соответствующую запись в конфигурации. [general] accessControlPlugin = "AccessControlPluginUser" С помощью параметра "ssaCertCheck" определяется необходимое имя для цепочки сертификатов, благодаря чему сертификат хоста признается действительным. В этом случае в сертификате должно присутствовать имя "root_SSA". Если имеется промежуточный центр сертификации, возможна следующая запись: ssaCertCheck = "chainPrefix=myETM_RootCA;myETM_IntermediateCA" В данном случае имеется корневой центр сертификации с общим именем " myAPDAR _RootCA" и промежуточный центр сертификации с именем " myAPDAR _IntermediateCA". При назначении этой записи все символы из конфигурационного файла должны присутствовать в сертификате. Например, если запись была задана следующим образом: "ssaCertCheck = "chainPrefix=my" Всё, что начинается со слова «my», является допустимым. Таким образом, это справедливо не только для myETM..., но и, например, для "myAPDAR..." и т. д.
[webClient] clientSideAuth = 0	Активирует аутентификацию на стороне сервера .
[ui] httpServer = "https://localhost:443"	Указывает веб-сервер и номер порта.

[general] ssaPrivateKey = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d ssaCertificate = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d ssaPrivateKey = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d7" ssaCertificate = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d7" ssaPrivateKey = "store:USER:MY:cn1" ssaCertificate = "store:USER:MY:cn1" ssaPrivateKey = "store:USER:MY:cn1" ssaCertificate = "store:USER:MY:cn1"	В записях указывается, какие сертификаты ищутся в хранилище сертификатов Windows. Здесь (см. рисунок слева) поиск сертификатов осуществляется по отпечатку. Если эти параметры конфигурации заданы в разделе [general] файла конфигурации, параметр sslChainFile может быть не задан, поскольку поиск сертификатов в хранилище сертификатов Windows не будет производиться. Здесь (см. рисунок слева) поиск сертификатов осуществляется по имени. В Windows хранилище сертификатов состоит из двух разделов: 1 - машина 2 - пользователь Если сертификат импортирован в машину, он становится доступен всем пользователям этой машины — мы рекомендуем именно такую настройку. В этом случае запись в конфигурации начинается с "store: MACHINE: ...". В случае, описанном с помощью "store: USER: ...", сертификаты доступны только для конкретного пользователя. Это различие необходимо указать в конфигурационном файле, чтобы поиск выполнялся в правильном хранилище.
[ctrl_5] ssaPrivateKey = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d7" ssaCertificate = "store:USER:MY:67 d6 90 fd 69 d3 ac a9 af 0d 25 3f 81 c0 df b8 09 94 17 d7" [ctrl_3] ssaPrivateKey = "store:USER:MY:cn1" ssaCertificate = "store:USER:MY:cn1" [ctrl_1] ssaPrivateKey = "file:root.key.pem" ssaCertificate = "file:root.cert.pem"	Если параметры конфигурации ssaPrivateKey и ssaCertificate заданы для разных менеджеров, эти менеджеры будут использовать другие сертификаты и ключи, чем в разделе [general].

Примечание:

Параметр ssaChainFile в конфигурации не требуется при использовании сертификатов из хранилища сертификатов Windows.

3.5. Действия при появлении ошибок

В случае ошибок отображаются ошибки, описанные ниже.

Сообщения об ошибках при аутентификации на стороне сервера для менеджеров

В журнале событий отображаются следующие сообщения об ошибках, связанные с аутентификацией на стороне сервера для менеджеров и привязкой сессий:

Сообщение об ошибке	Описание
WCCOActrl (5), 2017.11.30 11:30:46.236, PARAM,SEVERE, 96, Нет авторизации, AccessControlPlugin - setUserId()	Это сообщение об ошибке отображается, когда смена пользователя невозможна. Переключиться на другого пользователя может только пользователь root.
WCCILevent (0), 2017.11.30 11:17:53.646, SYS, SEVERE, 10/auth, незаконное сообщение от Manager (SYS: 1 Ctrl -num 2 CONN: 1) с идентификатором пользователя 3072, сообщение 1024 отключено	Если менеджер запускается от имени пользователя, отличного от указанного в сертификате, отображается это сообщение об ошибке. При аутентификации менеджеров на стороне сервера используется привязка сессии. При привязке сессии имя пользователя APDAR является частью сертификата.