|  |
| --- |
| Акционерный коммерческий Сберегательный Банк Российской Федерации(Открытое Акционерное Общество) |
| Sync Server  Настройка SSL для WebSphere AS |
| Руководство по установке |

## Настройка WebSphere Application Server

Следующие действия необходимо выполнить в административной консоли WebSphere Application Server.

Используйте существующий сервер или при необходимости создайте новый. После установки в WAS уже создан сервер приложений server1, который может быть использован для установки Системы.

## Создание серверного хранилища сертификатов

1. На странице [Защита](javascript:expandCollapse('17');) -> Управление сертификатами SSL и ключамивойдите в раздел Хранилища ключей и сертификаты
2. Нажмите кнопку Создать
3. Введите следующие данные  
   *Имя*: MisMobileServerKey  
   *Описание*: Серверный ключ для Mis Mobile Server  
   *Путь*: укажите любой путь на файловой системе, где будут храниться ваши серверные сертификаты. *Пример:* *${CONFIG\_ROOT}/cells/MR-32009-00151Node01Cell/nodes/MR-32009-00151Node01/m*isMobileServer*.jks  
   Пароль:* любой пароль (123456) *Подтверждение:* подтверждение  
   *Тип:* JKS
4. Установите галочку Инициализировать при запуске и проверьте, что галочки Только чтение и Включить аппаратную обработку операций отключены
5. Нажмите Применить.
6. Выберите подраздел Личные сертификаты
7. Если предполагается создать и использовать свой собственный сертификат (self-signed certificate)
   1. Нажимаем Создать -> Собственный сертификат.
   2. Введите следующие данные  
      *Псевдоним:* server  
      *Размер ключа:* 1024  
      *Срок действия:* 1825
   3. Заполните оставшиеся поля информацией о компании и системе
   4. Нажимаем OK
8. Если северный сертификат представлен в хранилище ключей
   1. Нажимаем Импортировать
   2. Выбираем Файл хранилища ключей
   3. В поле Имя файла ключей вводим локальный путь до хранилища с ключами
   4. Выбираем тип хранилища и вводим пароль
   5. Нажимаем Получить псевдонимы файла ключей
   6. Выбираем необходимый псевдоним
   7. В поле Псевдоним импортированного сертификата указываем значение Server
   8. Нажимаем OK
9. Вернитесь на страницу с сертификатом, нажав на MisMobileServerKey
10. Выберите подраздел Сертификаты подписантов
11. Выделите все сертификаты и удалите их.

## Создание хранилища для проверки клиентских сертификатов

1. На странице [Защита](javascript:expandCollapse('17');) -> Управление сертификатами SSL и ключамивойдите в раздел Хранилища ключей и сертификаты
2. Нажмите кнопку Создать
3. Введите следующие данные  
   *Имя*: MisMobileServerTrustStore   
   *Описание*: Хранилище доверенных сертификатов для Mis Mobile Server  
   *Путь*: укажите любой путь на файловой системе, где будут храниться ваши серверные сертификаты. *Пример:* *${CONFIG\_ROOT}/cells/MR-32009-00151Node01Cell/nodes/MR-32009-00151Node01/m*isMobileServerTrust*.jks  
   Пароль:* любой пароль *Подтверждение:* подтверждение  
   *Тип:* JKS
4. Установите галочку Инициализировать при запуске и проверьте, что галочки Только чтение и Включить аппаратную обработку операций отключены
5. Нажмите Применить.
6. Выберите подраздел Сертификаты подписантов
7. Нажмите кнопку Добавить
8. Введите данные  
   *Псевдоним:* Sberbank root ca  
   *Имя файла:* Путь до файла сертификата sberbank\_root.cer   
   *Тип данных:* Текстовые данные в кодировке Base64
9. Нажмите кнопку *Применить*
10. Нажмите кнопку *Добавить*
11. Введите данные  
    *Псевдоним:* Sberbank external ca  
    *Имя файла:* Путь до файла sberbank\_ca.cer из дистрибутива  
    *Тип данных:* Текстовые данные в кодировке Base64
12. Выделите все кроме только что созданных сертификатов, и удалите их.

## Создание SSL-конфигурации

1. На странице [Защита](javascript:expandCollapse('17');) -> Управление сертификатами SSL и ключамивойдите в раздел Конфигурации SSL
2. Нажмите на кнопку Создать
3. Введите данные  
   *Имя:* MisMobileServerConfig   
   *Имя надежного хранилища:* MisMobileServerTrustStore  
   *Имя хранилища ключей:* MisMobileServerKey
4. Нажмите на кнопку Получить псевдонимы сертификатов
5. Задайте следующие данные  
   *Псевдоним по умолчанию сертификата сервера:* Server  
   *Псевдоним по умолчанию сертификата клиента:* Server
6. Нажмите кнопку Применить
7. Войдите подраздел Параметры качества защиты QoP
8. Установите параметр Идентификация клиента в значение Обязательные. Нажмите кнопку OK

## Установка SSL-конфигурации

1. Зайдите на страницу Управление сертификатами SSL и ключами -> Управлять конфигурациями защиты конечных точек
2. В дереве раскройте Входящие -> <Имя ячейки, где будет работать приложение> -> nodes -> <Имя ноды, где будет работать приложение> -> servers
3. Нажмите на имя сервера.
4. В блоке Конкретная конфигурация SSL для этой конечной точки отметьте галочку Переопределить унаследованные значения
5. В поле Конфигурация SSL выберите **MisMobileServerConfig**
6. Нажмите на кнопку Обновить список псевдонимов сертификатов.
7. Псевдоним сертификата в хранилище ключей выберите server
8. Повторите шаги 2-7 заменив ветку Входящие на Исходящие
9. *Сохраните изсенения*
10. *Перезапустите WebSphere AS*
11. Проверьте функционирование приложения открыв в браузере   
    <https://hostname:port/mis_syncserver>\_context\_path  
    где hostname – доменное имя (или IP-адрес) WAS,

port – SSL порт (по умолчанию 9443),

mis\_syncserver\_context\_path – контекст приложения, указанный при установке для war-файла