

3.1.1.4 Настройка доступа к защищенному веб-сайту по предъявлению токена

Раздел содержит инструкцию по настройке доступа к защищенному веб-сайту по предъявлению токена.

Для настройки необходим компьютер с установленной операционной системой **Windows 2012 R2 Server Rus**, драйверами **Рутокен** и опубликованный в IIS **веб-сайт**, для которого будет производиться настройка аппаратной аутентификации. ОС должна быть настроена как **веб-сервер**. В системе должны быть установлены **Службы сертификации**.

Пользователям должны быть выданы сертификаты типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.

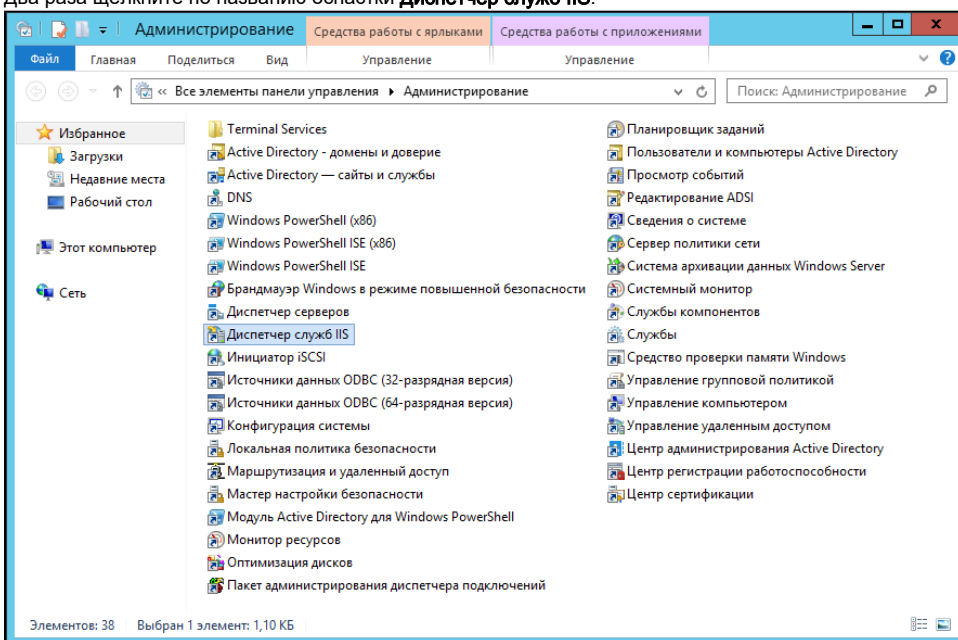
Все описанные далее действия должны производиться с правами администратора системы.

Для примера будет использована веб-директория **Outlook Web Access** на сайте **веб-узел по умолчанию**.

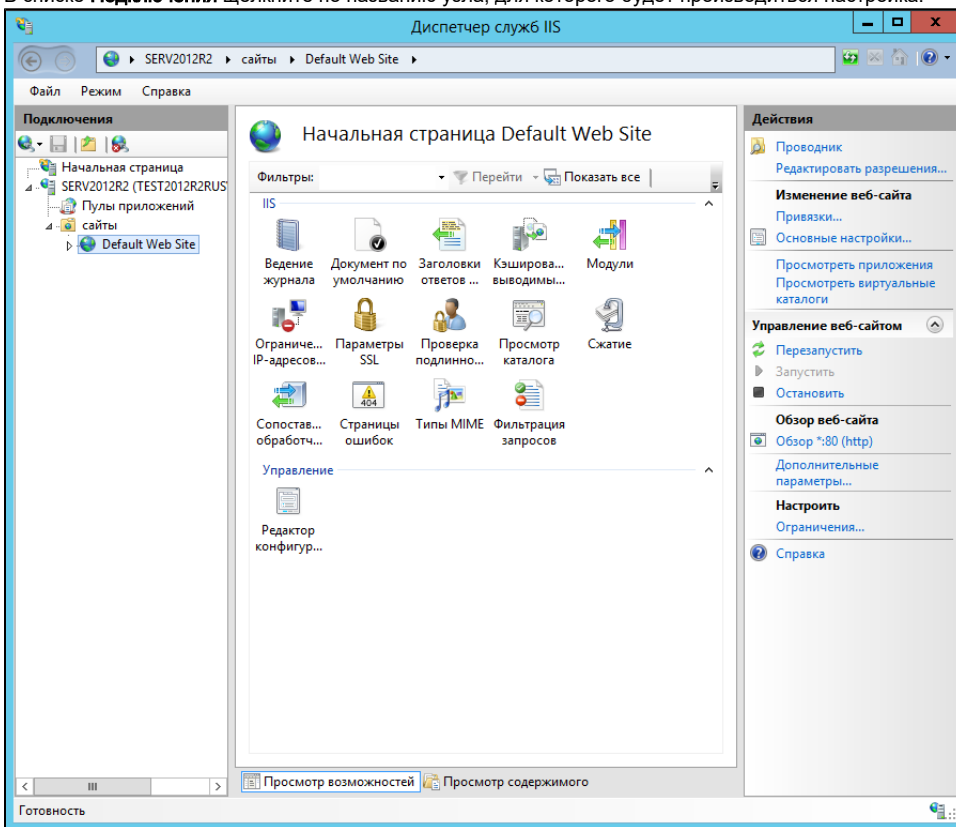
Настройки будут проводиться с правами учетной записи **Admin**.

Для настройки параметров безопасности веб-сайта:

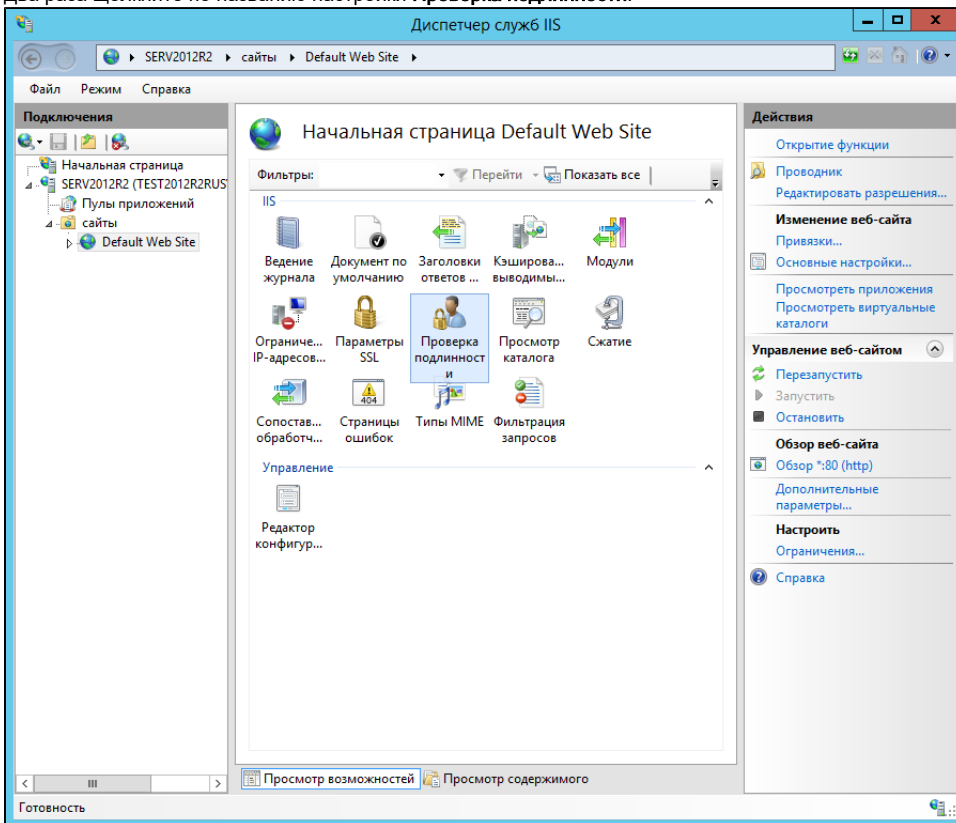
1. Откройте **Панель управления**.
2. Введите в поле поиска название пункта **Администрирование**.
3. Два раза щелкните по названию оснастки **Диспетчер служб IIS**.



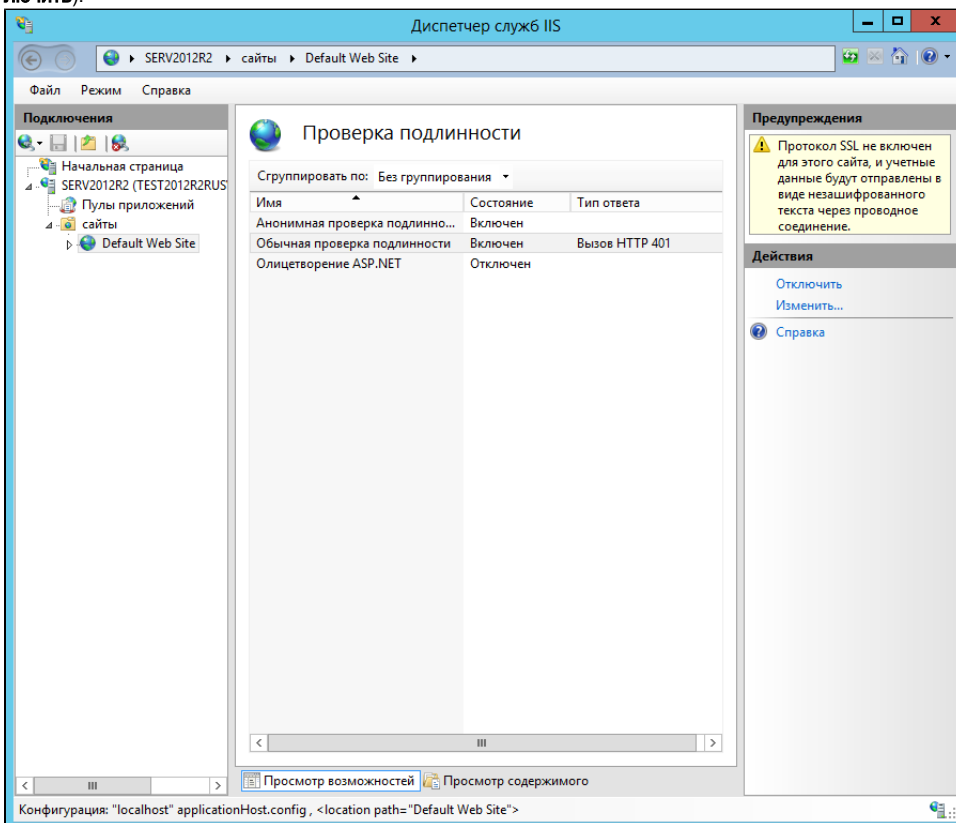
4. В списке **Подключения** щелкните по названию узла, для которого будет производиться настройка.



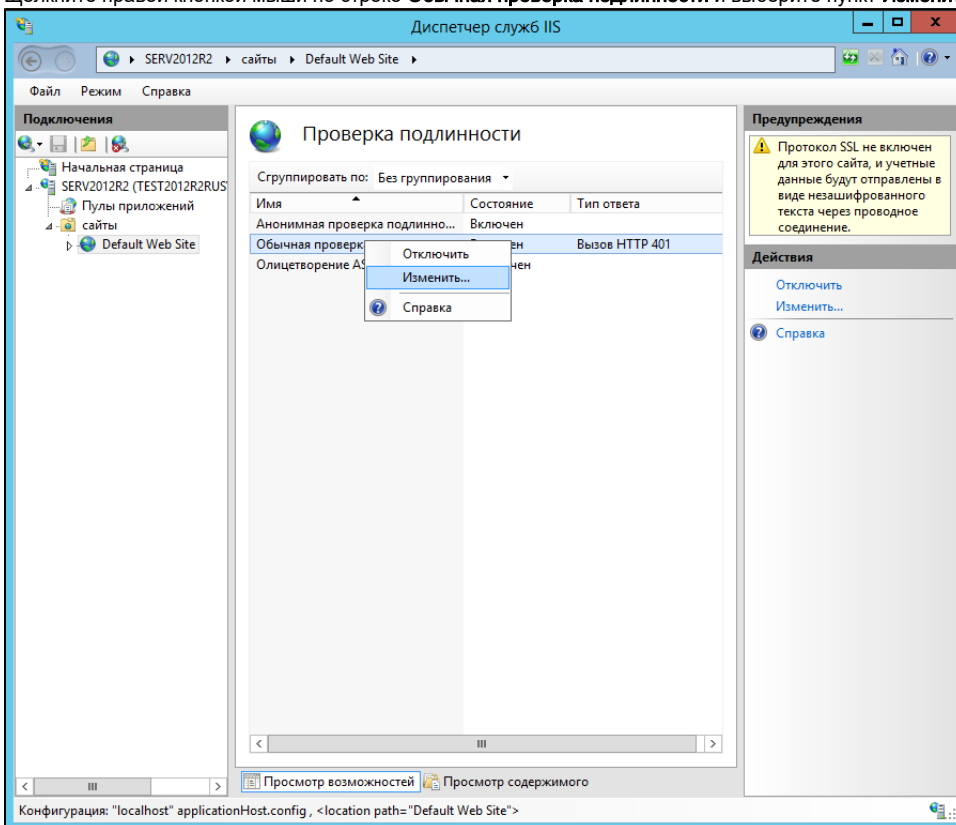
5. Два раза щелкните по названию настройки **Проверка подлинности**.



6. Если базовая аутентификация отключена, то включите ее (щелкните по строке **Обычная проверка подлинности** и щелкните по ссылке **Включить**).

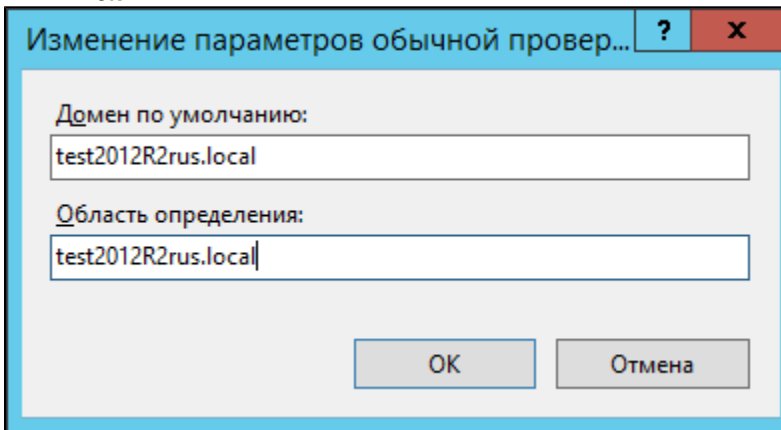


7. Щелкните правой кнопкой мыши по строке **Обычная проверка подлинности** и выберите пункт **Изменить...**

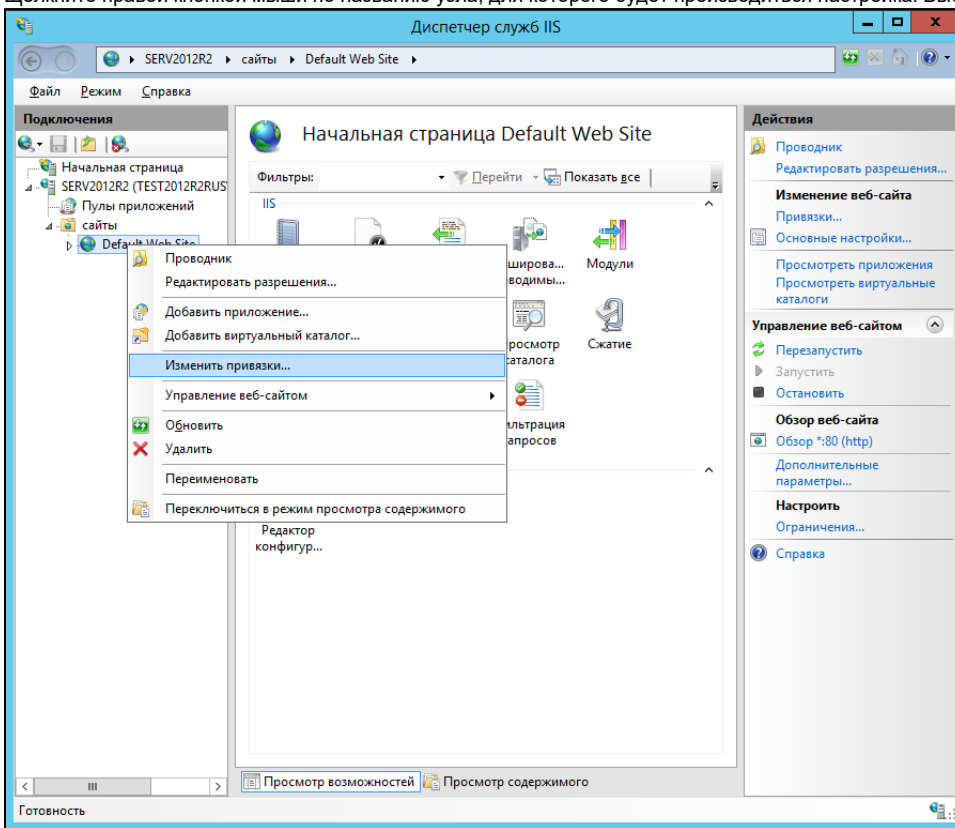


8. Укажите название домена, в котором расположен веб-сервер.

9. Нажмите **ОК**.



10. Щелкните правой кнопкой мыши по названию узла, для которого будет производиться настройка. Выберите пункт **Изменить привязки...**



11. В окне **Привязки сайта** нажмите **Добавить**.

Тип	Имя узла	Порт	IP-адреса	Сведения о при...
http		80	*	

Buttons: **Добавить...**, **Изменить...**, **Удалить**, **Обзор**, **Закреть**

12. В раскрывающемся списке **Тип** выберите значение **https**.

Fields: **Тип:** https, **IP-адрес:** Все неназначенные, **Порт:** 443, **Имя узла:** [empty], ☐ **Требовать обозначение имени сервера**, **SSL-сертификат:** Не выбрано, **Выбрать...**, **Вид...**, **OK**, **Отмена**

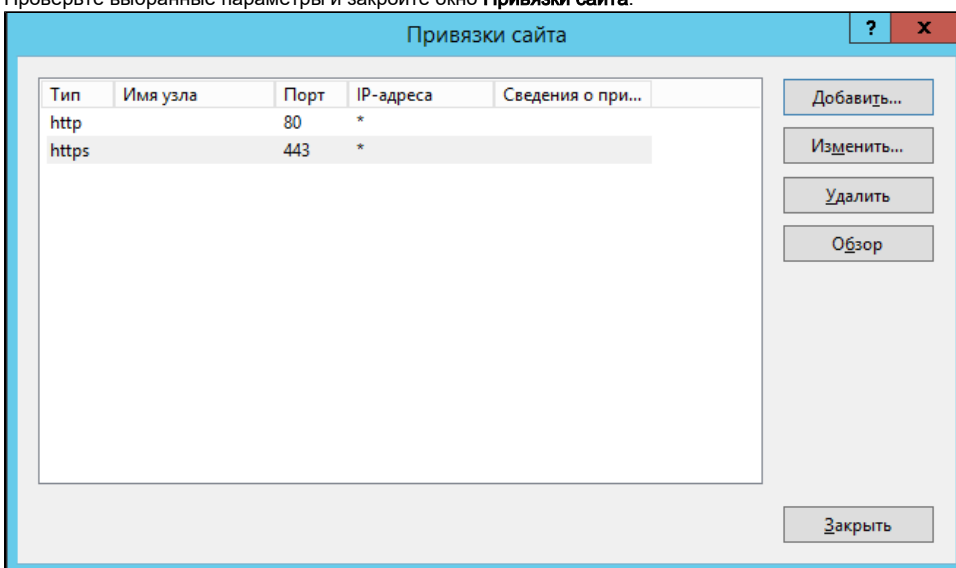
13. В раскрывающемся списке **SSL-сертификат** выберите сертификат, который будет использоваться в аутентификации веб-сервера. Нажмите **OK**.

Fields: **Тип:** https, **IP-адрес:** Все неназначенные, **Порт:** 443, **Имя узла:** [empty], ☐ **Требовать обозначение имени сервера**, **SSL-сертификат:** [dropdown menu open], **Выбрать...**, **Вид...**, **OK**, **Отмена**

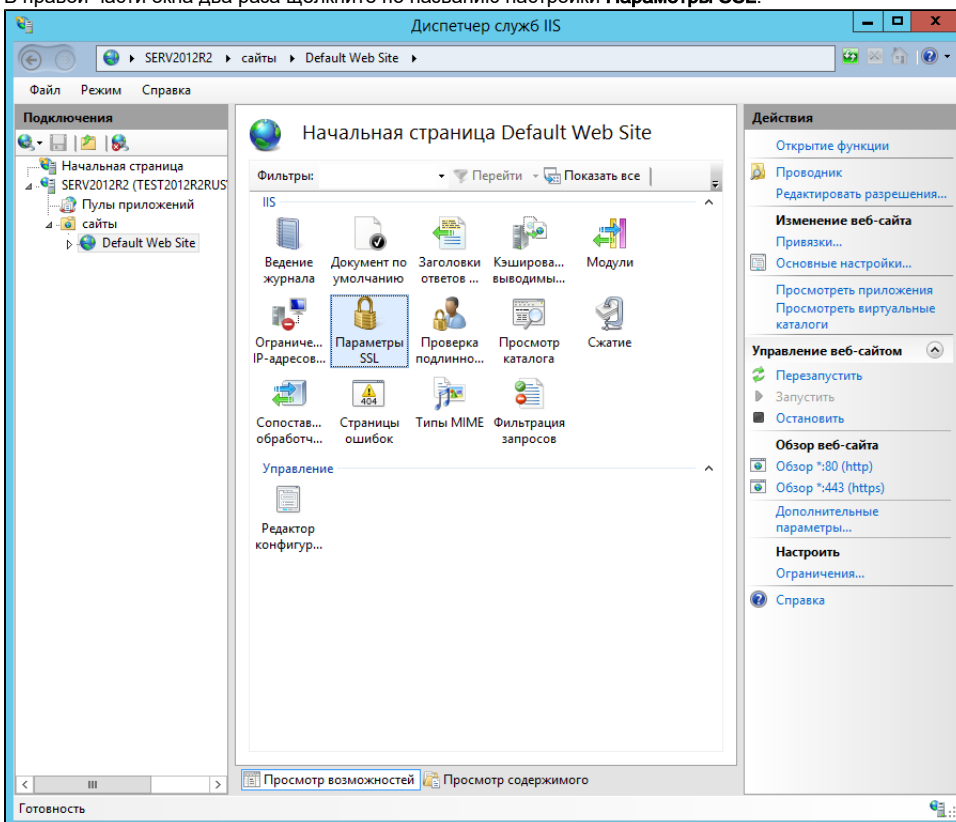
SSL-сертификат dropdown options:

- Не выбрано
- Не выбрано
- Serv2012R2.test2012R2rus.local
- test2012R2rus-SERV2012R2-CA

14. Проверьте выбранные параметры и закройте окно **Привязки сайта**.

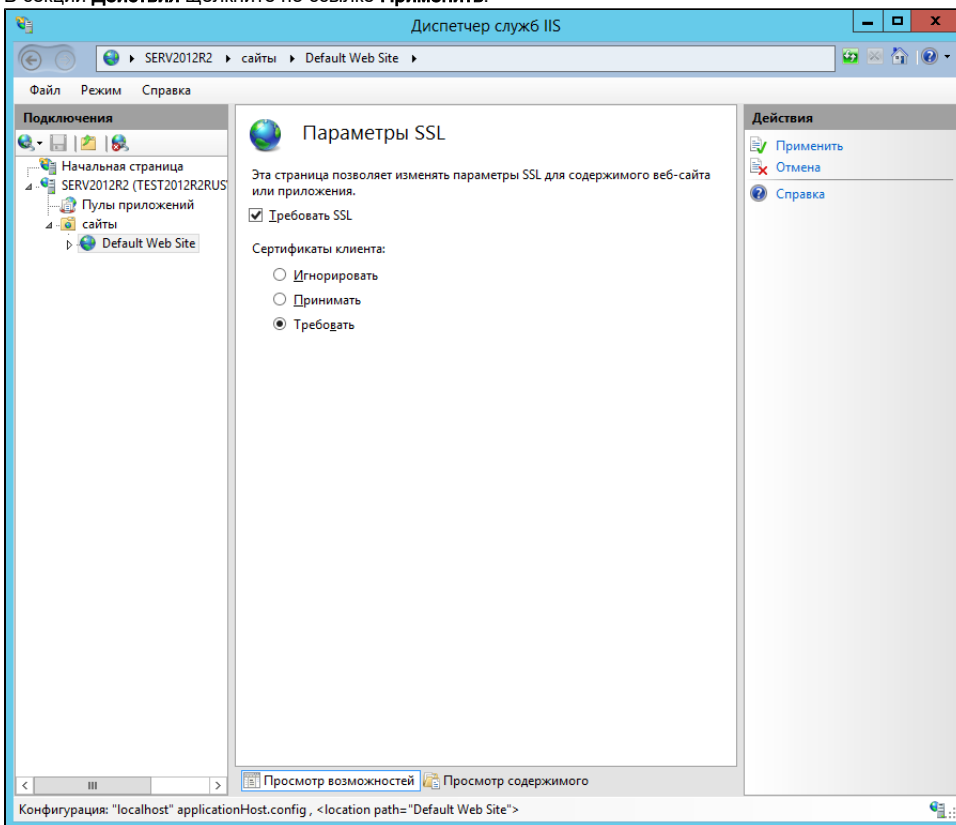


15. В правой части окна два раза щелкните по названию настройки **Параметры SSL**.



16. В секции **Параметры SSL** установите флажок **Требовать SSL** и переключатель в положение **Требовать**.

17. В секции **Действия** щелкните по ссылке **Применить**.



На этом настройка безопасности веб-сервера закончена. Далее следует настроить подключение к защищенному веб-сайте **на клиентском компьютере**.