

3.1.2.4 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 2016 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**.

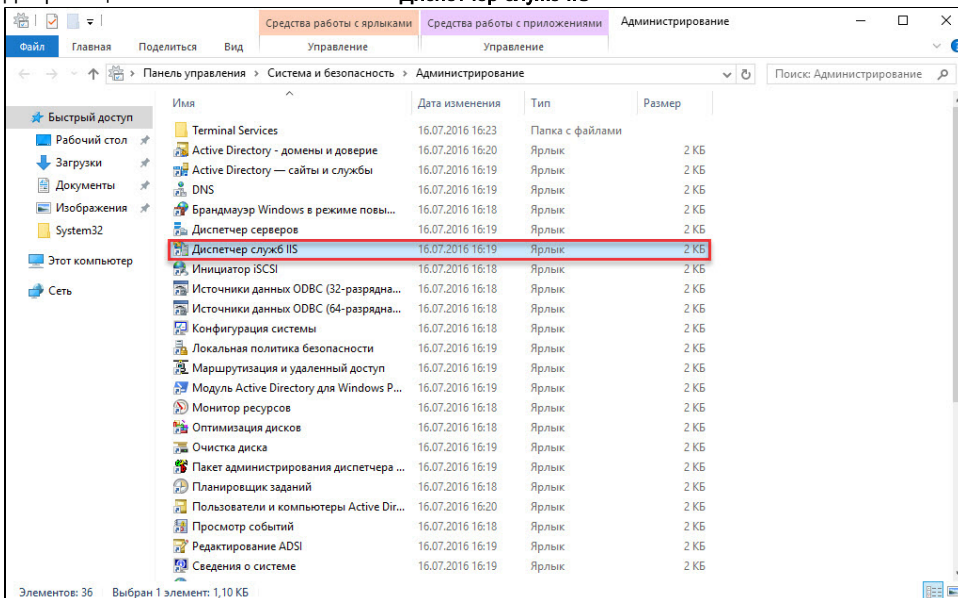
Все описанные далее действия должны производиться с правами администратора системы.

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

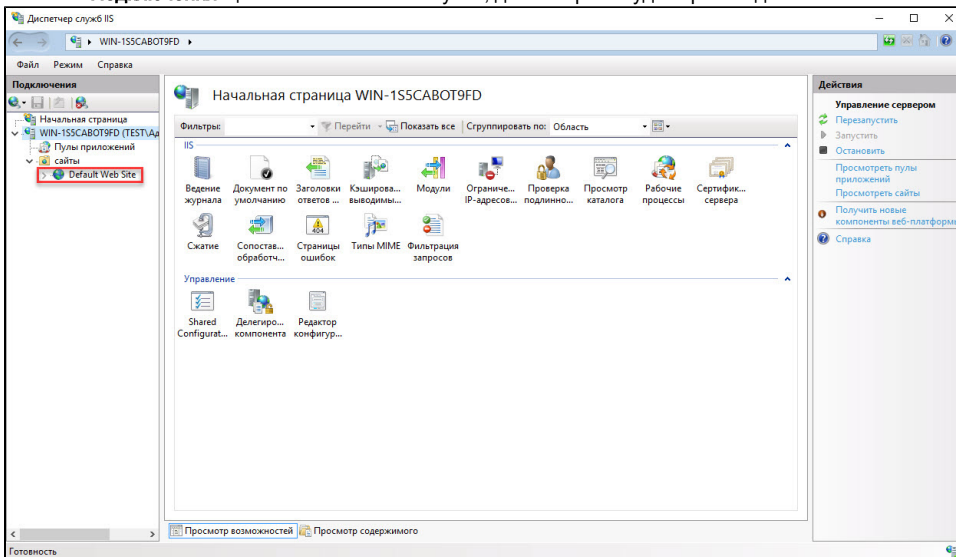
Настройки будут проводиться с правами учетной записи **Admin**.

Для настройки параметров безопасности веб-сайта:

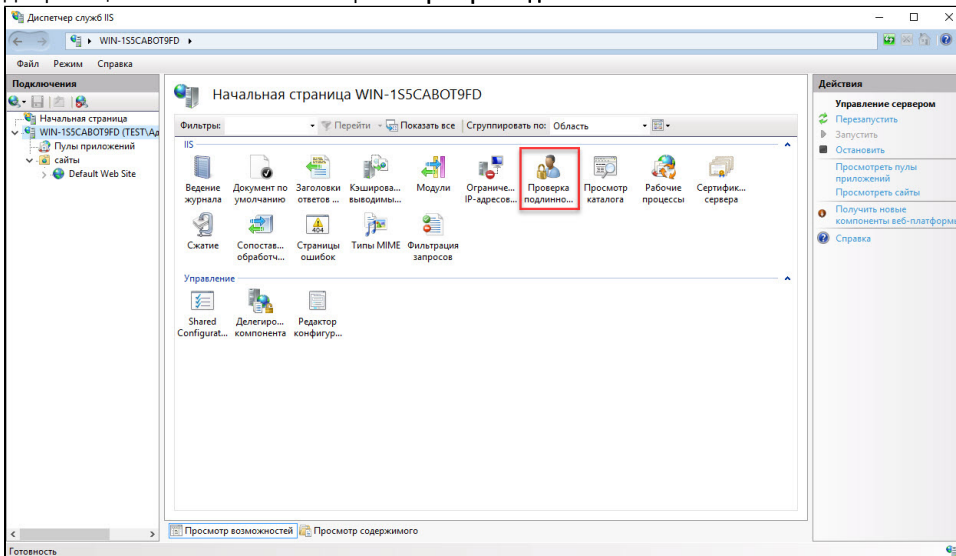
1. Откройте **Панель управления**.
2. В поле поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.
4. Два раза щелкните по названию оснастки **Диспетчер служб IIS**.



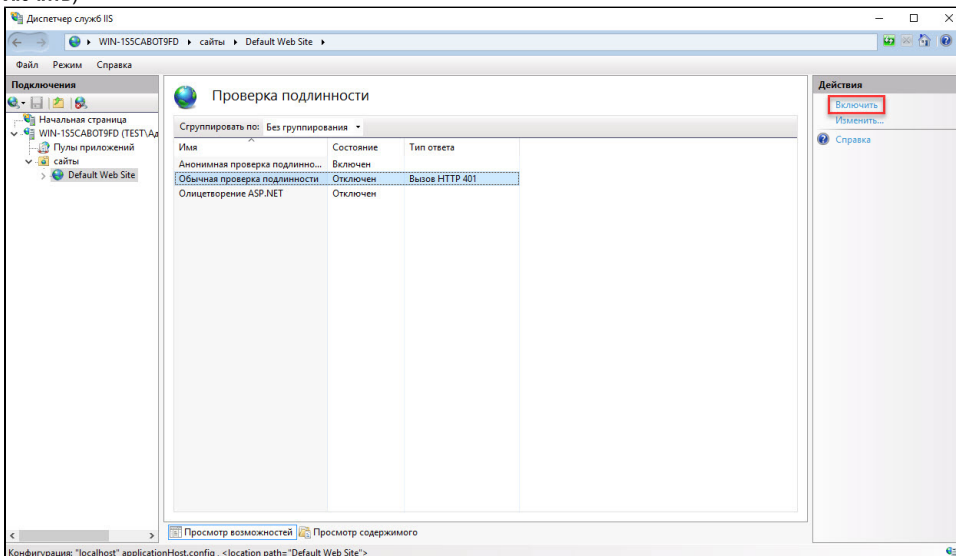
5. В списке **Подключения** щелкните по названию узла, для которого будет производиться настройка.



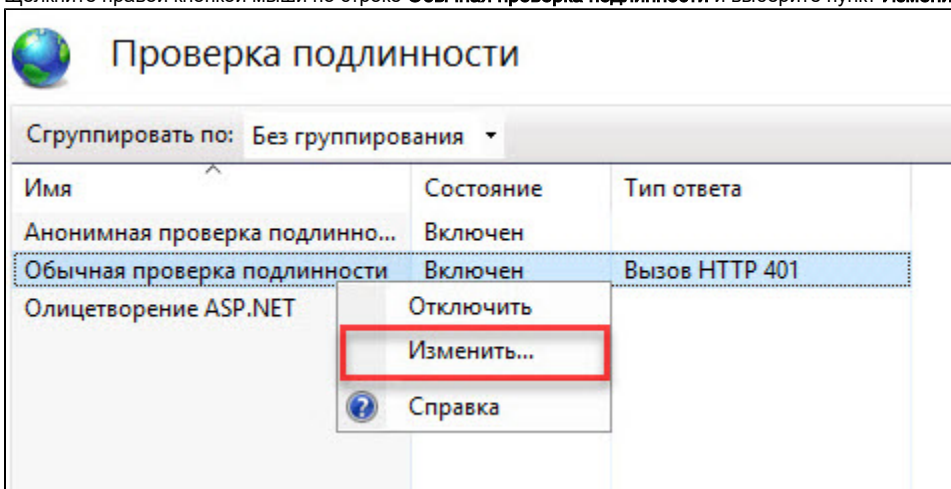
6. Два раза щелкните по названию настройки **Проверка подлинности**.



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

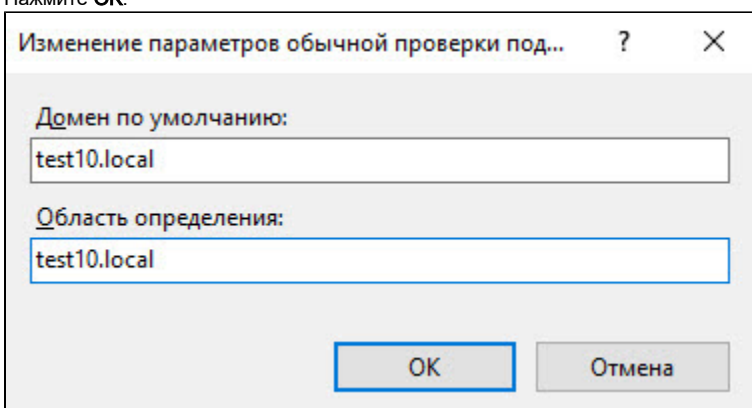


8. Щелкните правой кнопкой мыши по строке **Обычная проверка подлинности** и выберите пункт **Изменить...**

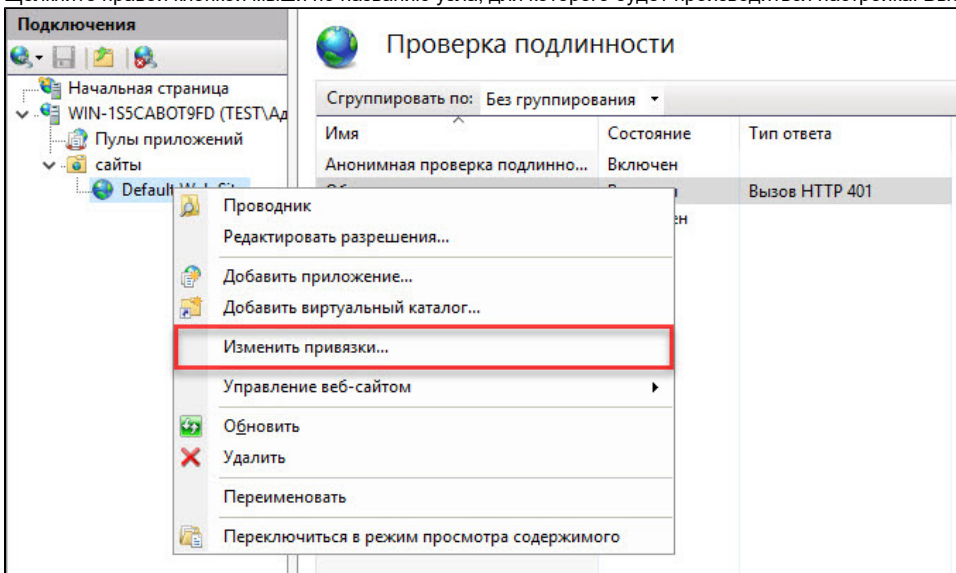


9. Укажите название домена, в котором расположен веб-сервер.

10. Нажмите **ОК**.



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



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

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

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

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

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

Тип: **1** **https** IP-адрес: Все неназначенные Порт: 443

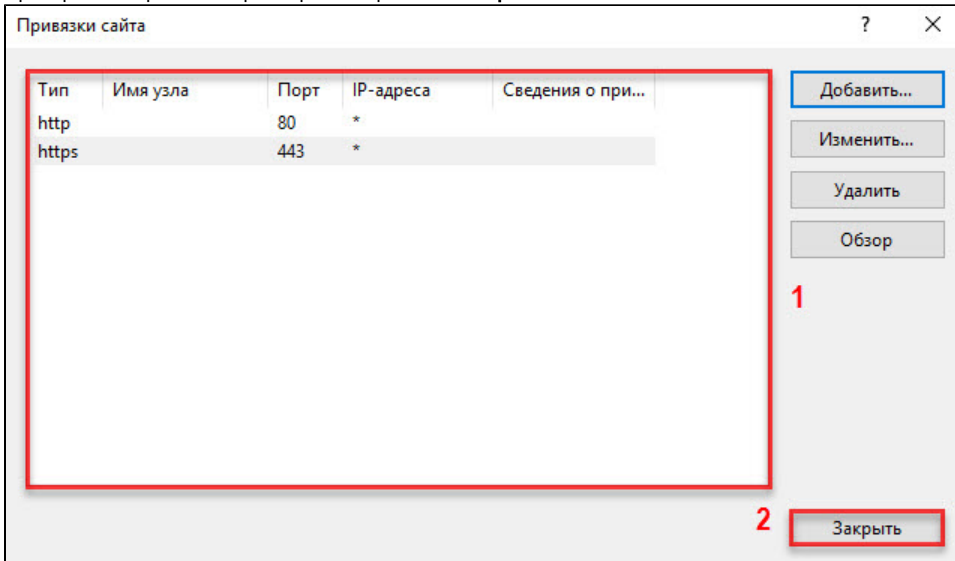
Имя узла:

☐ Требовать обозначение имени сервера

SSL-сертификат: **2** **test-WIN-1S5CABOT9FD-CA** **3** **OK**

Buttons: Выбрать..., Вид..., Отмена

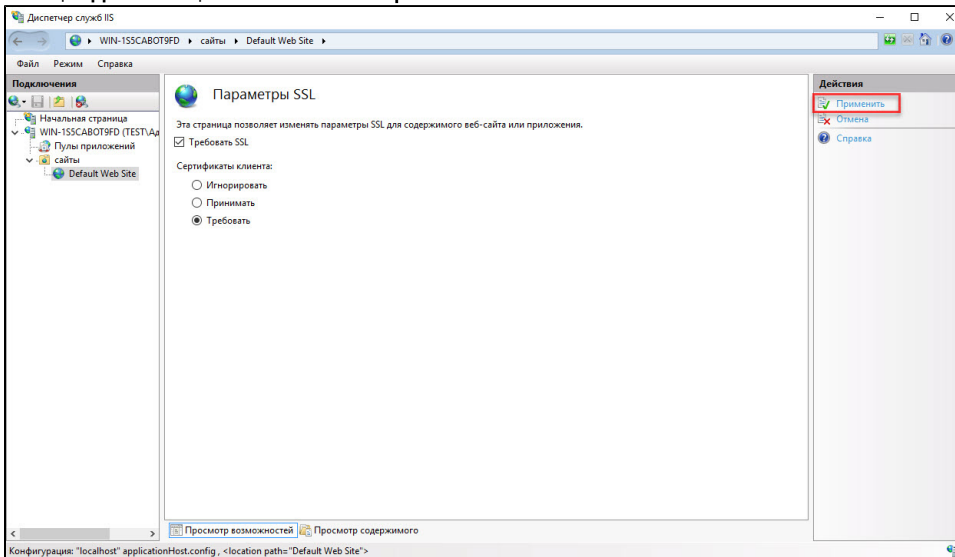
15. Проверьте выбранные параметры и закройте окно **Привязки сайта**.



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

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

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



На этом настройка безопасности веб-сервера закончена. Далее следует настроить подключение к защищенному веб-сайту [на клиентском компьютере](#).

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

Для настройки необходим компьютер с установленной операционной системой **Windows 2016 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.

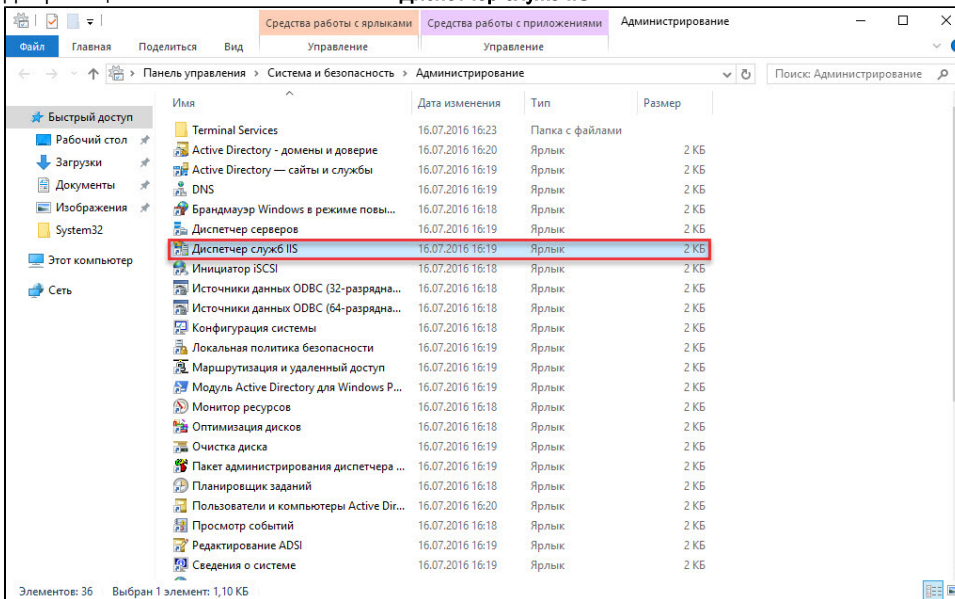
Для примера будет использована веб-директория **Outlook Web Access** на сайте **веб-узел по умолчанию**.

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

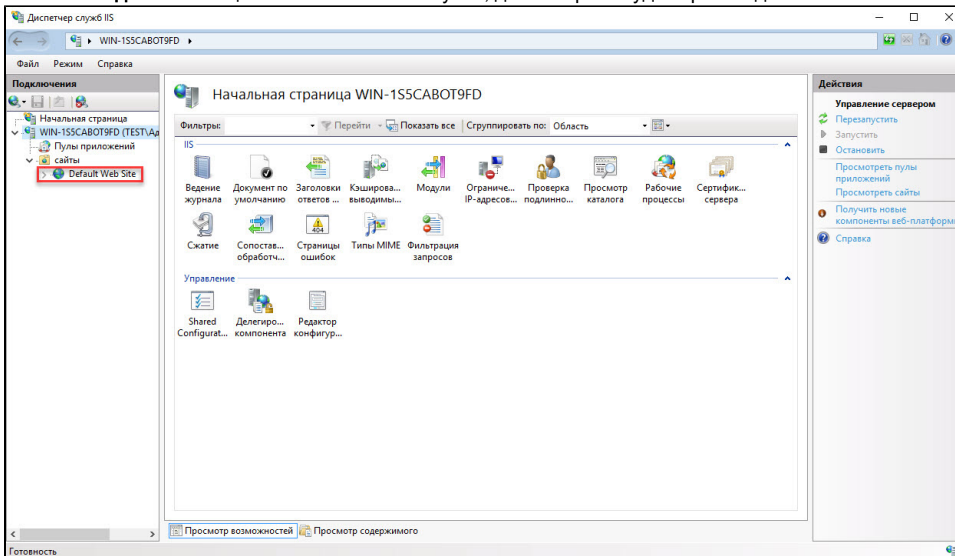
Для настройки параметров безопасности веб-сайта:

1. Откройте **Панель управления**.
2. В поле поиска введите слово "администрирование".
3. Два раза щелкните по названию пункта **Администрирование**.

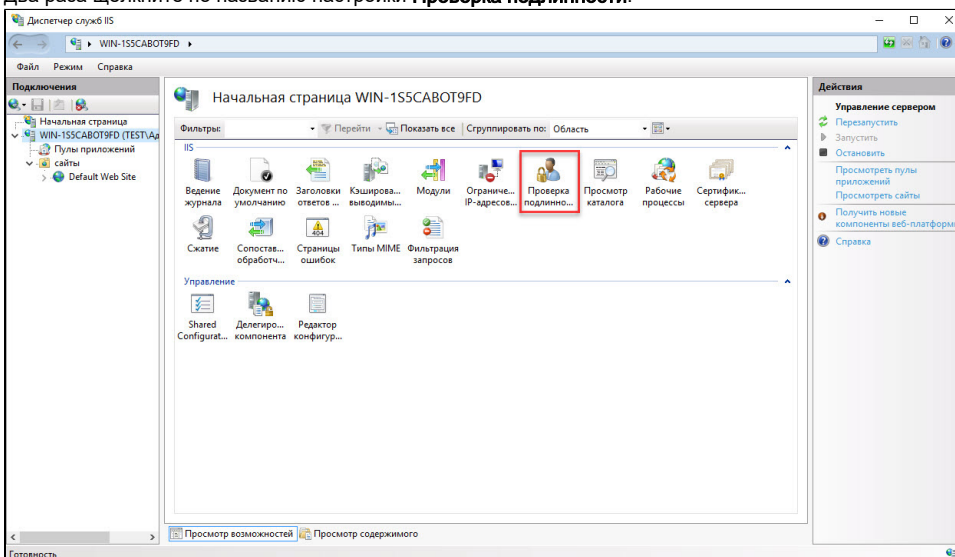
4. Два раза щелкните по названию оснастки **Диспетчер служб IIS**.



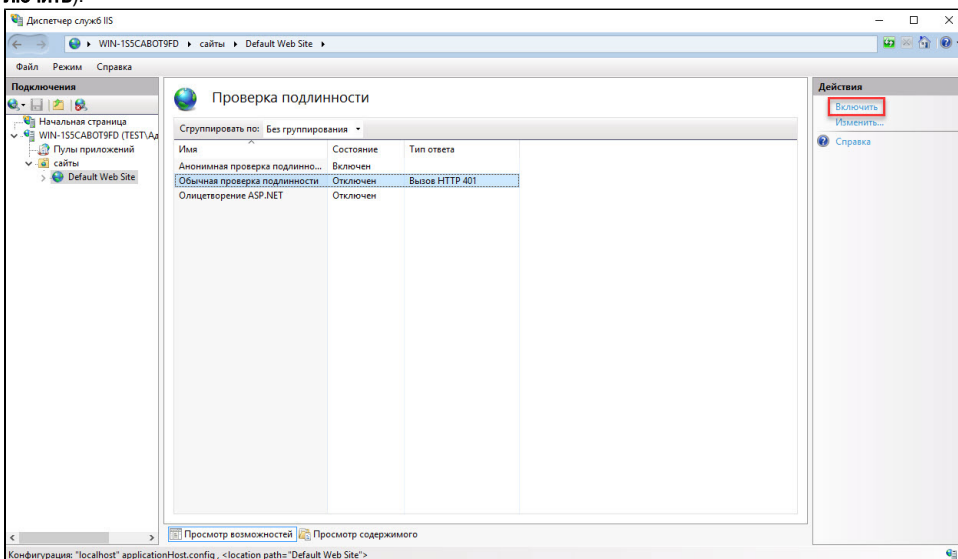
5. В списке **Подключения** щелкните по названию узла, для которого будет производиться настройка.



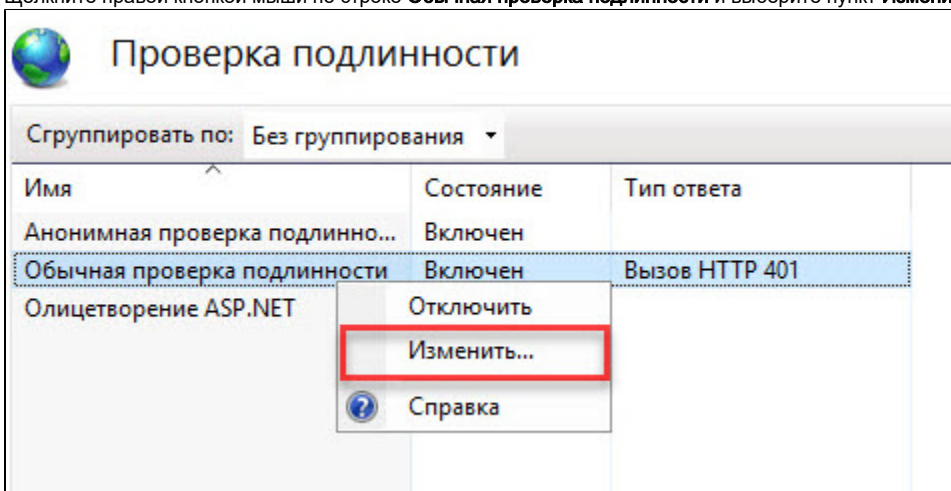
6. Два раза щелкните по названию настройки **Проверка подлинности**.



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

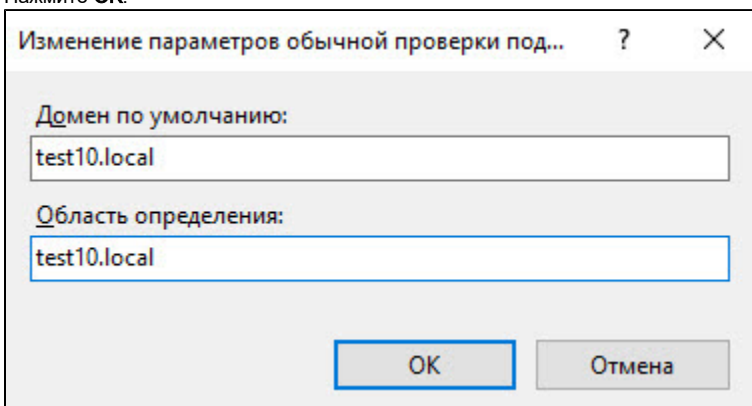


8. Щелкните правой кнопкой мыши по строке **Обычная проверка подлинности** и выберите пункт **Изменить...**

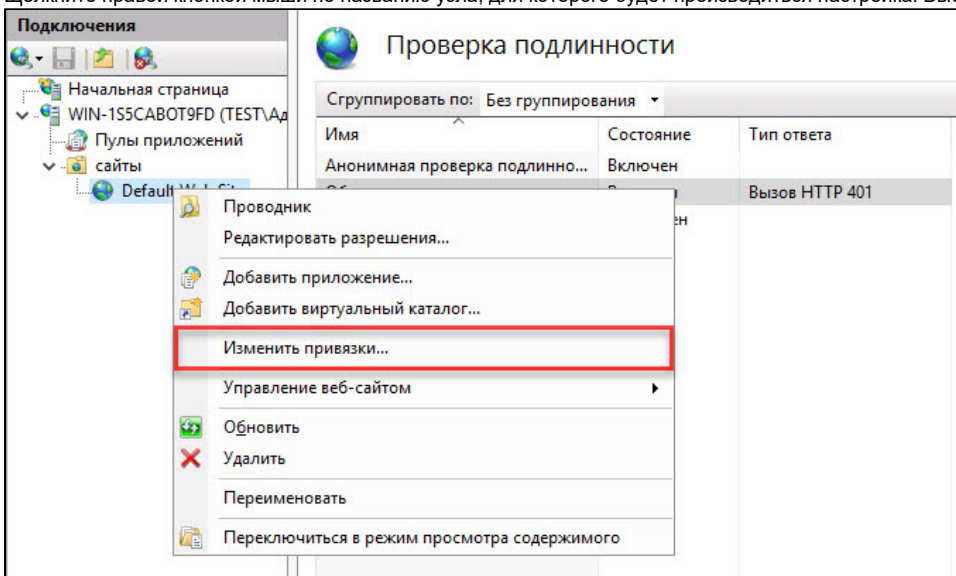


9. Укажите название домена, в котором расположен веб-сервер.

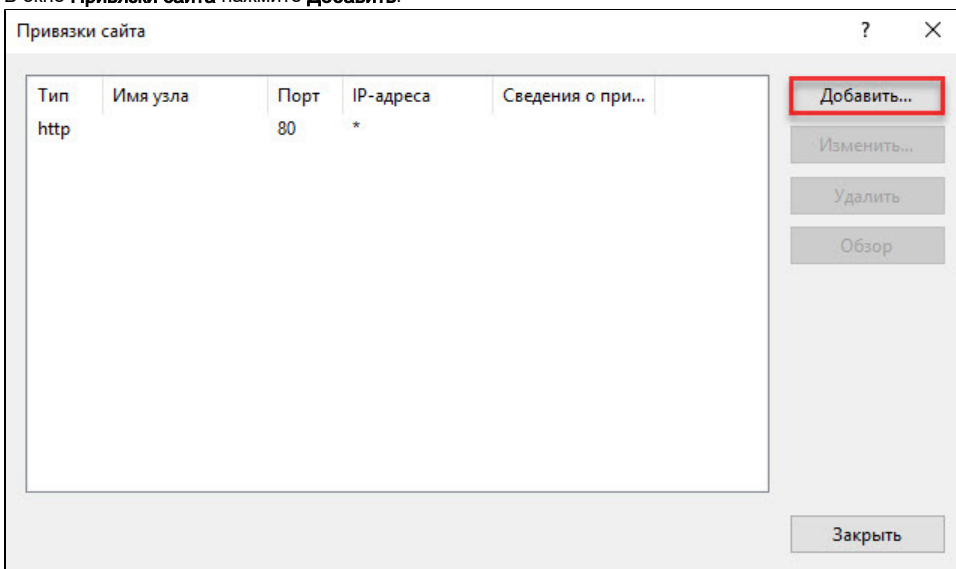
10. Нажмите **ОК**.



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



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



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

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

Добавление привязки сайта

Тип: **https** IP-адрес: Все неназначенные Порт: 443

Имя узла:

☐ Требовать обозначение имени сервера

SSL-сертификат: **test-WIN-1S5CABOT9FD-CA** Выбрать... Вид...

ОК Отмена

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

Привязки сайта

Тип	Имя узла	Порт	IP-адреса	Сведения о при...
http		80	*	
https		443	*	

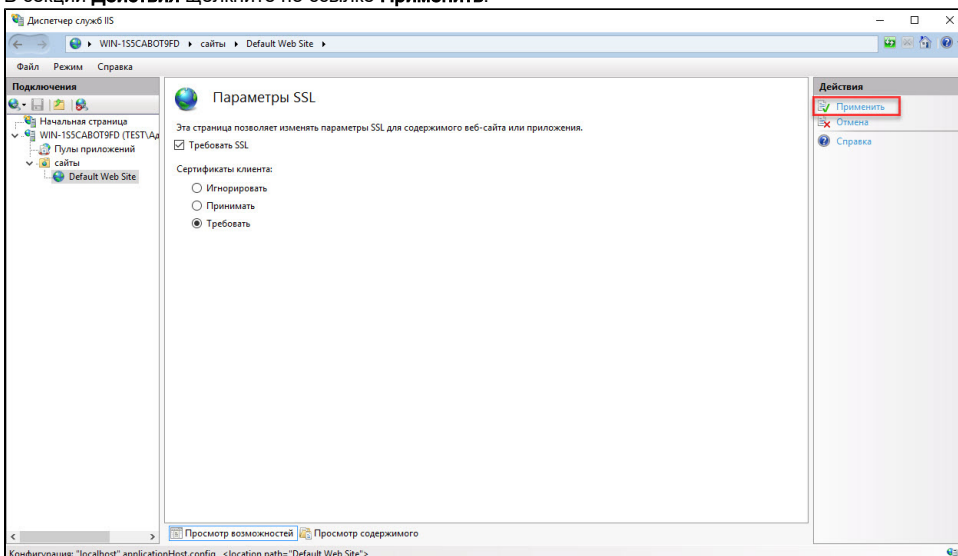
Добавить... Изменить... Удалить Обзор

Закреть

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

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

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



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