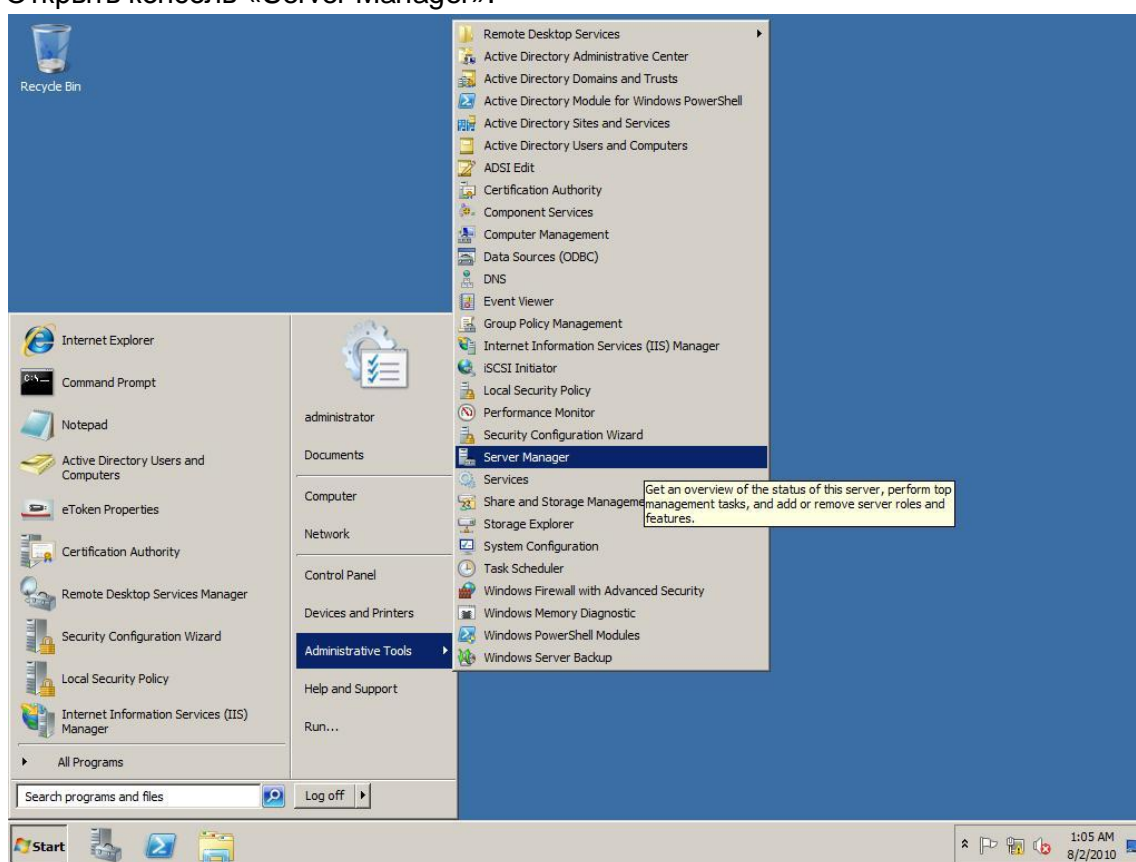


Настройка тонкого клиента ТОНК с MS WinCE6 для работы с Windows Server 2008 Terminal Server.

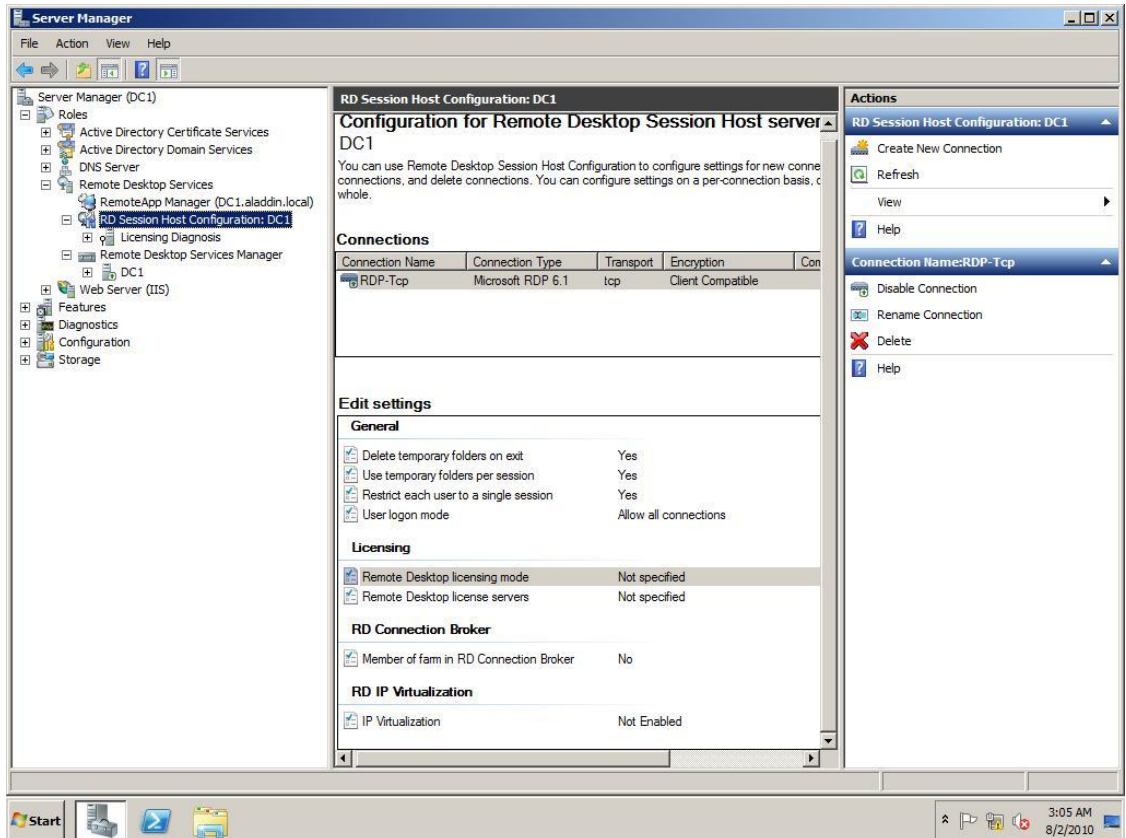
В MS Windows Server 2008 в Terminal Services изменился процесс аутентификации пользователей и устройств при подключении к RDP сессии – появился ряд нововведений. Одним из них является Network Layer Authentication, которое позволяет аутентифицировать клиента до установления полнофункциональной RDP сессии. Однако операционные системы семейства MS Windows Compact Embedded не поддерживают сценарий Network Layer Authentication с применением цифровых сертификатов, в связи с этим на терминальном сервере функцию Network Layer Authentication необходимо отключить.

Для того чтобы отключить NLA на сервере MS Windows Server 2008 Terminal Server необходимо:

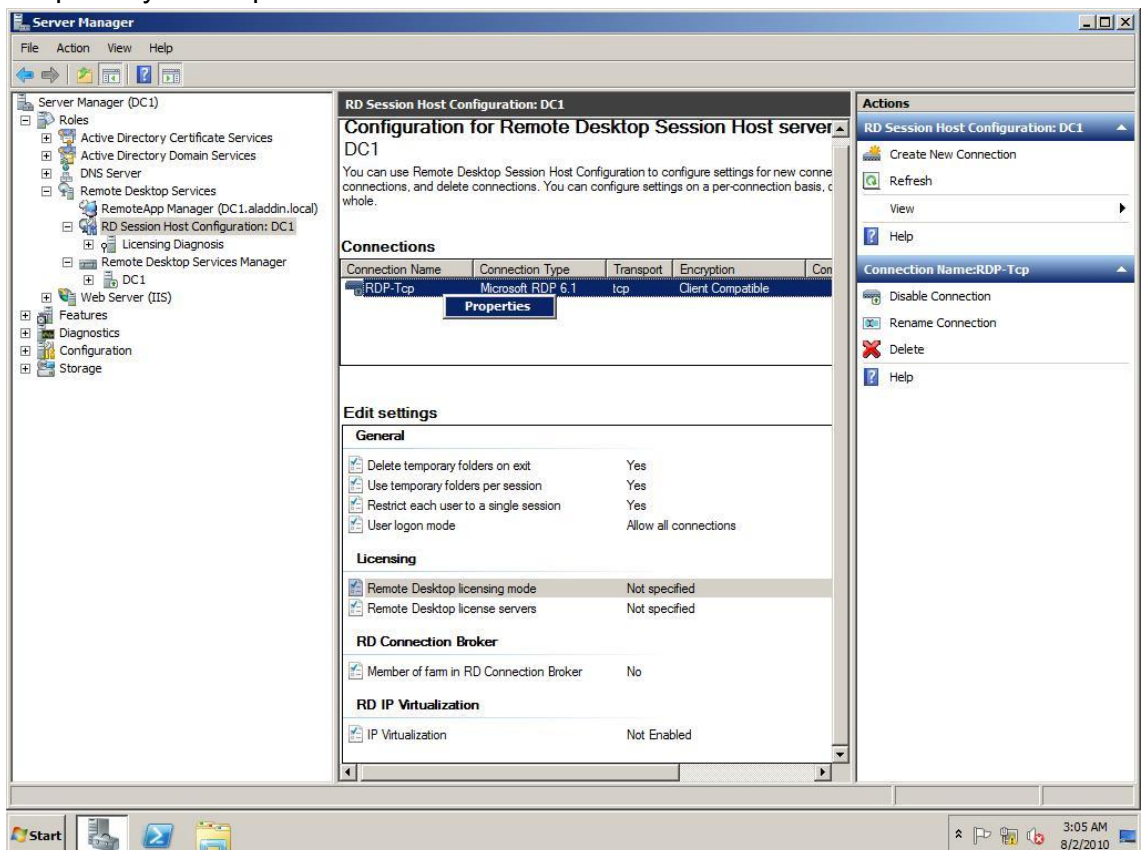
1. Открыть консоль «Server Manager».



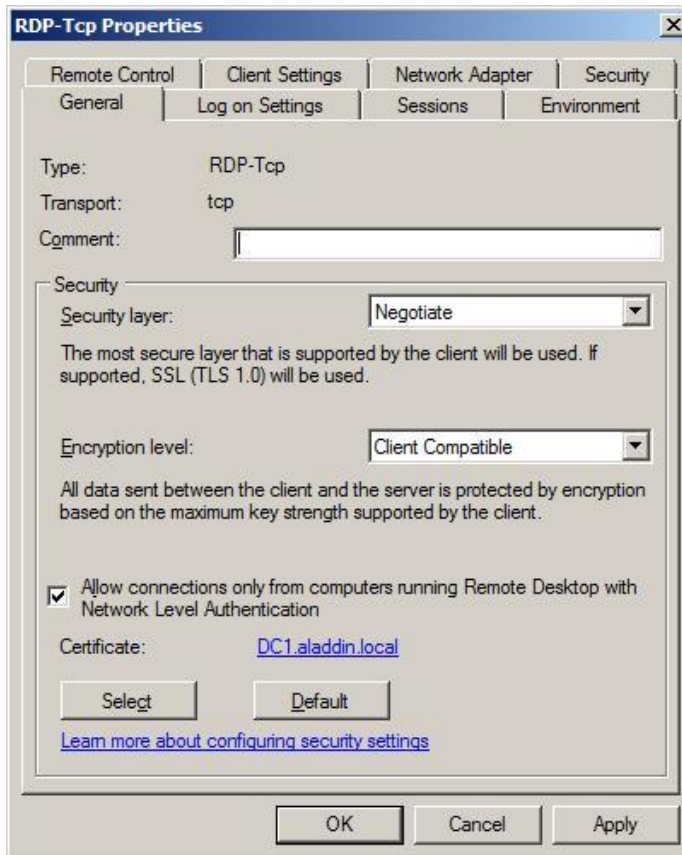
2. В консоли Service Manager в левой части экрана раскрыть дерево Roles->Remote Desktop Services->RD Session Host Configuration: <ComputerName>.



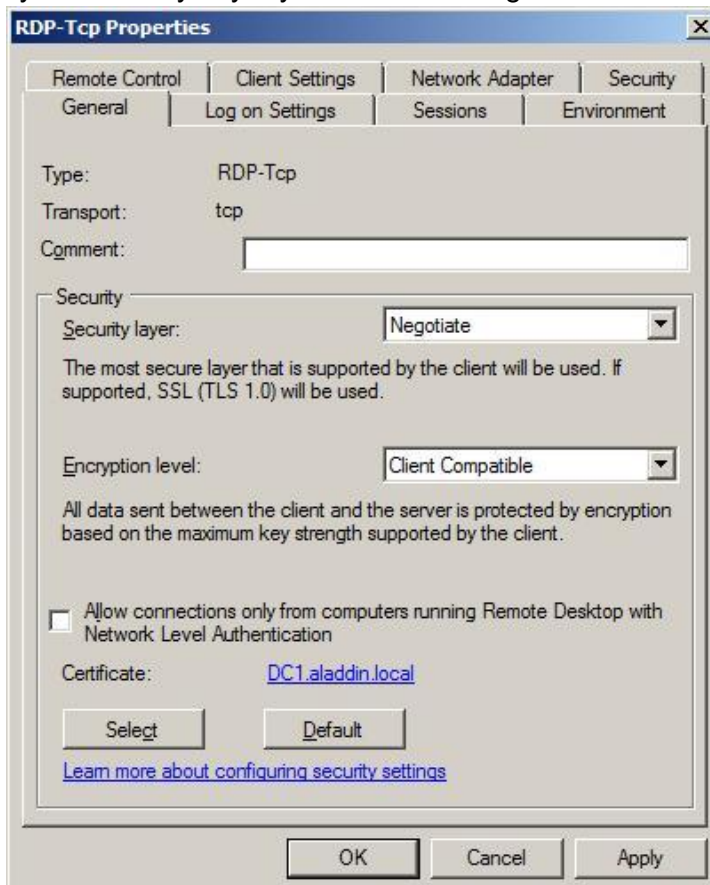
3. В консоли Service Manager в левой части экрана выбрать пункт RD Session Host Configuration: <Computer Name>, затем в рабочей средней части экрана нажатием правой кнопки мыши на пункте RDP-Tcp вызвать контекстное меню и из него выбрать пункт Properties.



4. В открывшемся окне RDP-Tcp Properties перейти на вкладку General.



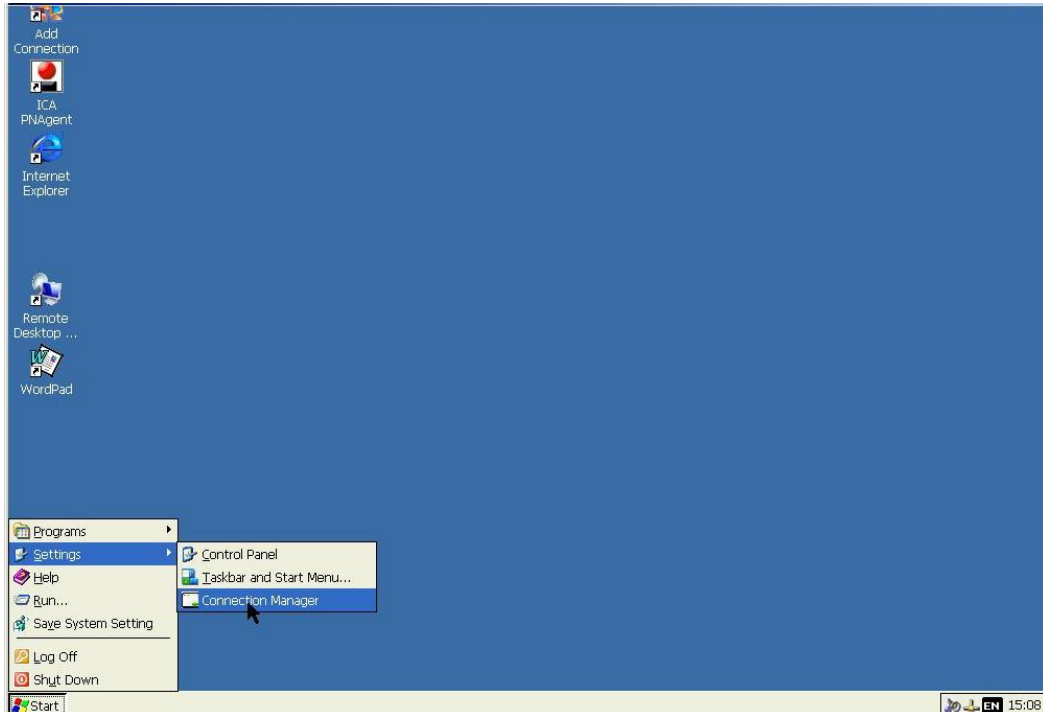
5. На вкладке General снять отметку «Allow connections only from computers running Remote Desktop with Network Layer Authentication». При этом нужно убедиться, что пункт Security Layer установлен в Negotiate.



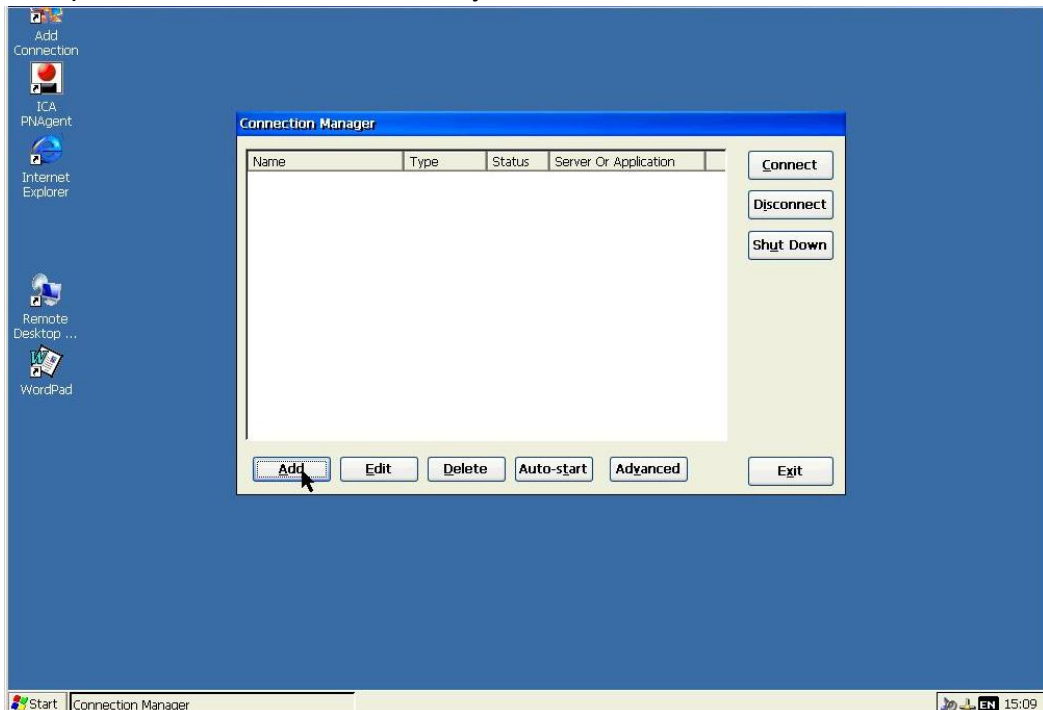
6. Нажать Ok. Настройка сервера завершена.

Как правильно настроить аутентификацию на MS Windows Server 2008 Terminal Server с тонкого клиента, работающего под управлением MS Windows CE6:

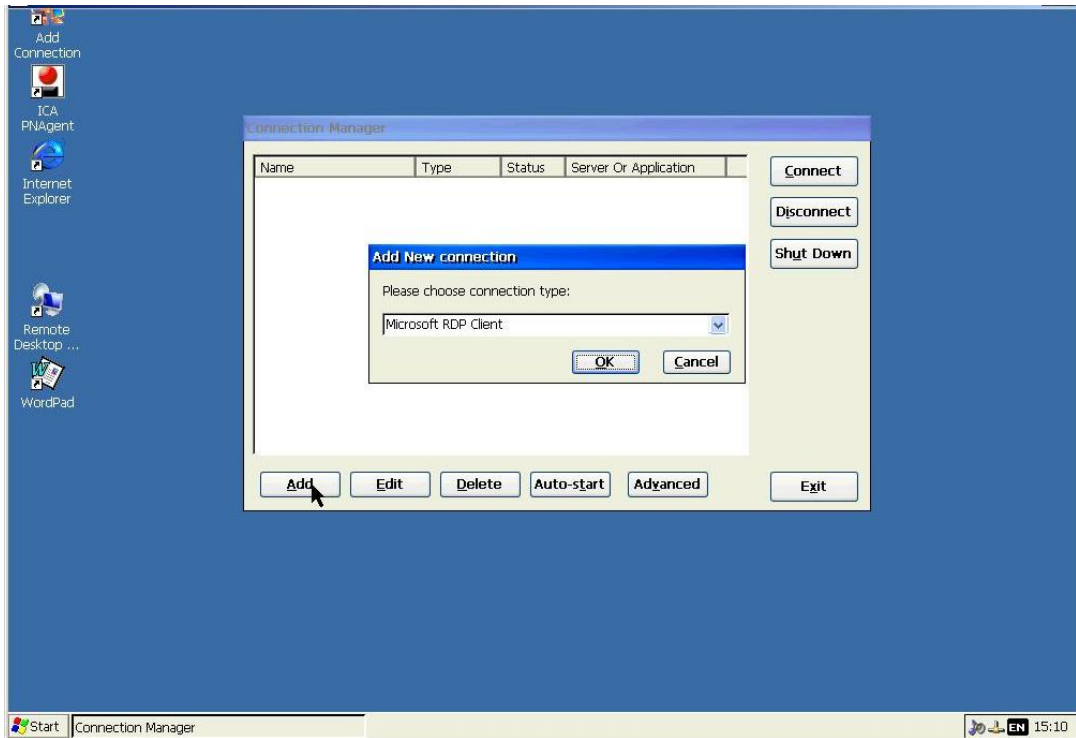
1. Запустить Connection Manager, для этого выбрать Start->Settings->Connection Manager.



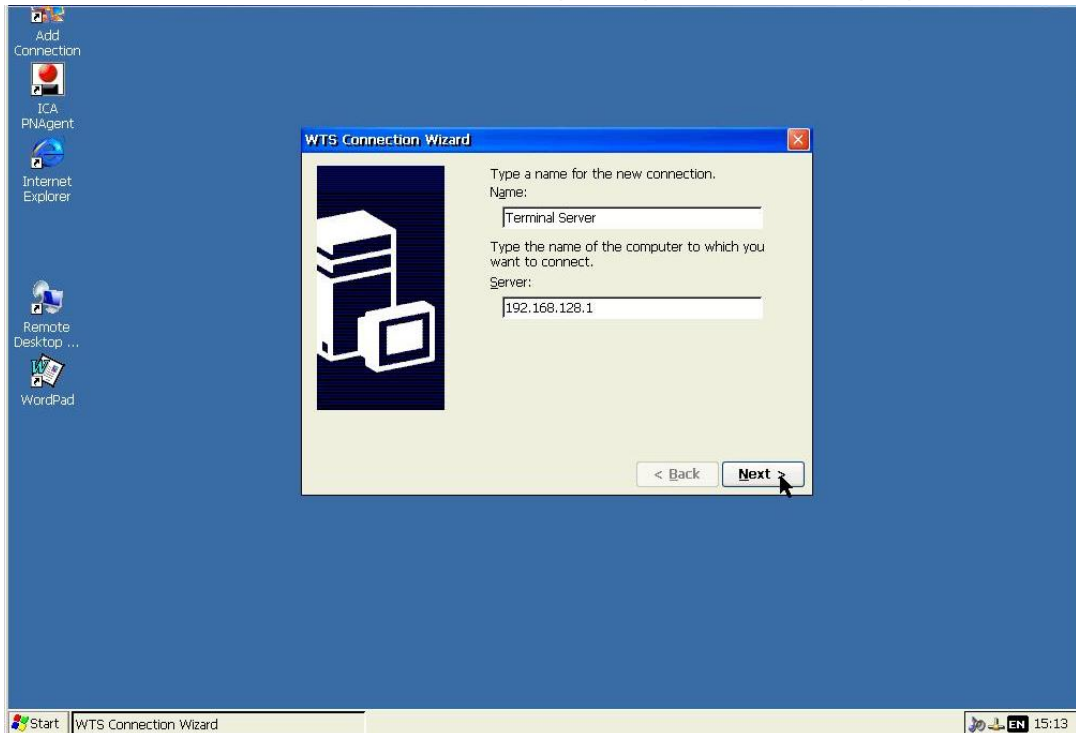
2. В открывшемся окне нажать кнопку Add.



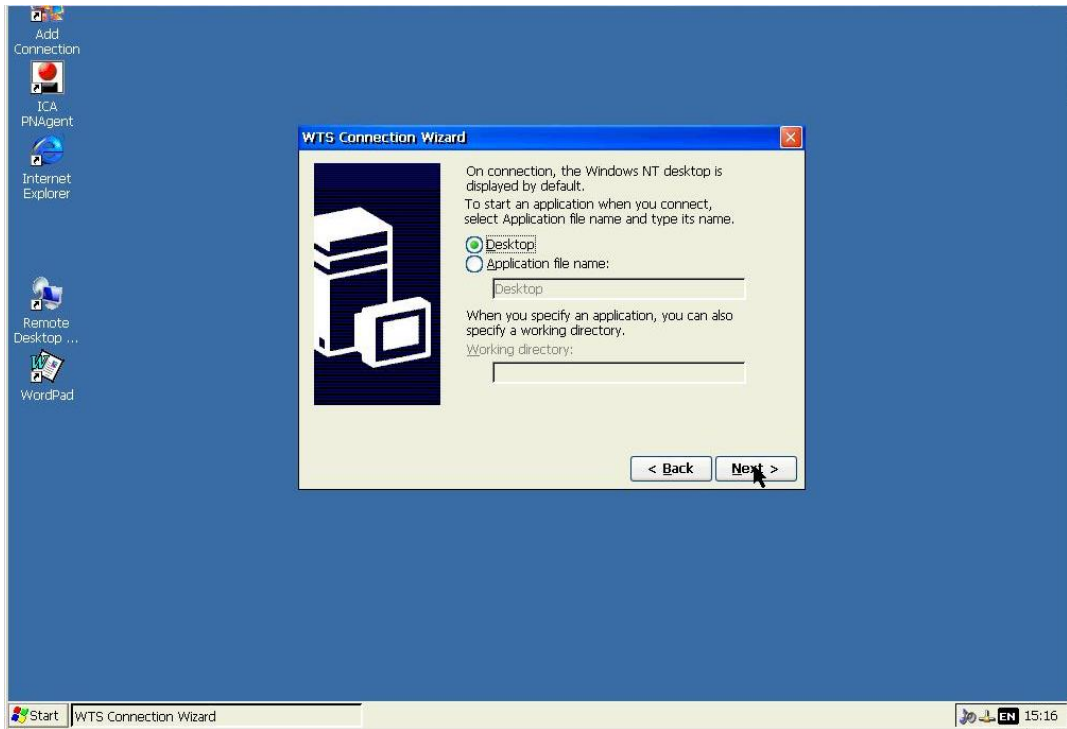
3. Далее в выпадающем списке выбрать Microsoft RDP Client и нажать Ok.



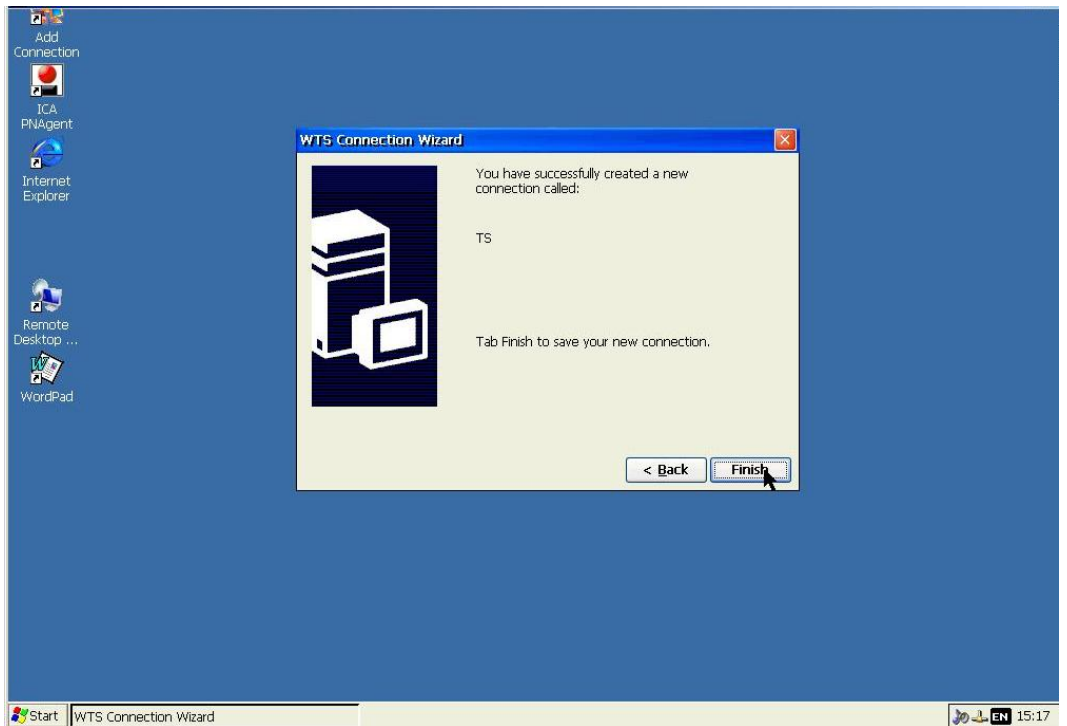
4. Указать имя соединения и имя или IP адрес терминального сервера и нажать Next.



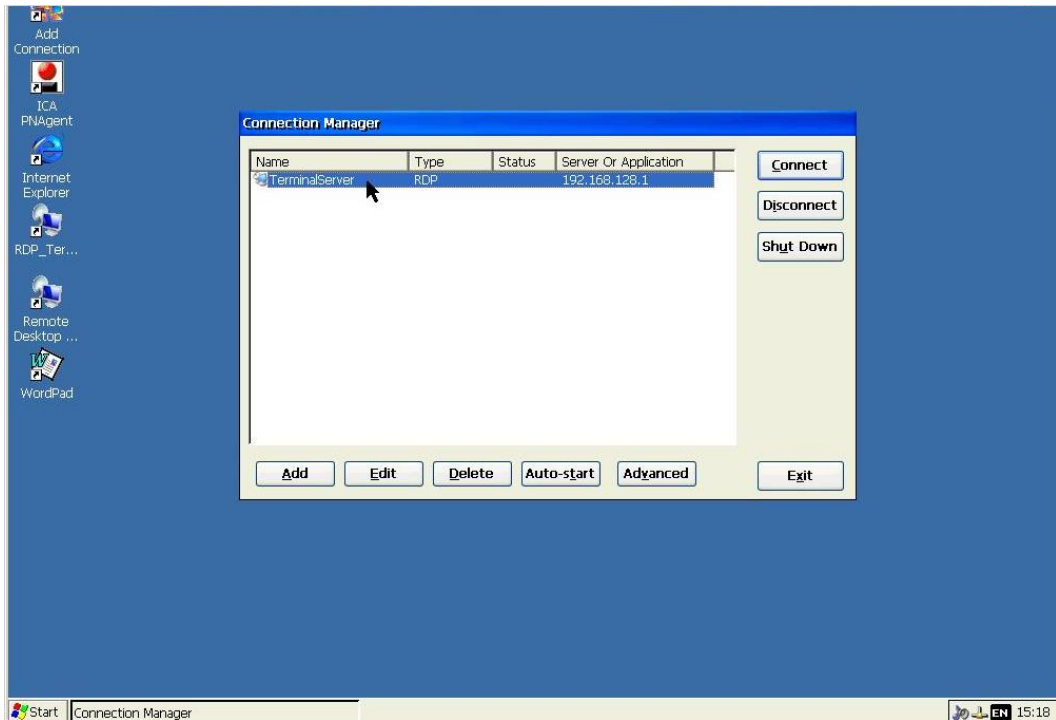
5. Выбрать пункт Desktop, нажать Next.



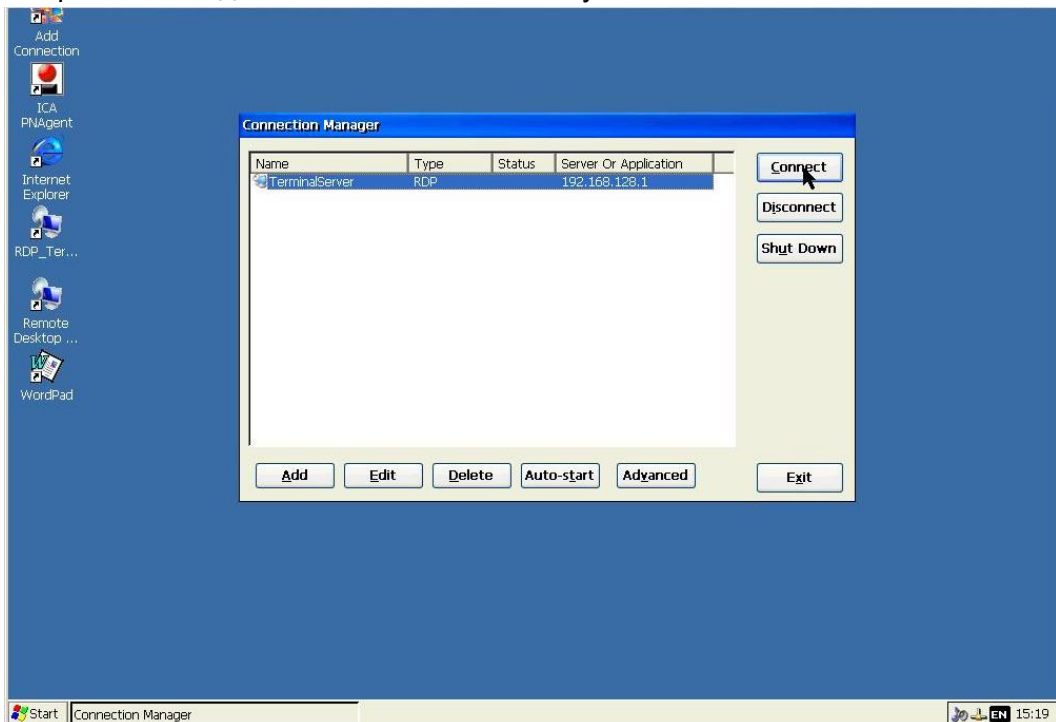
6. Нажать Finish.



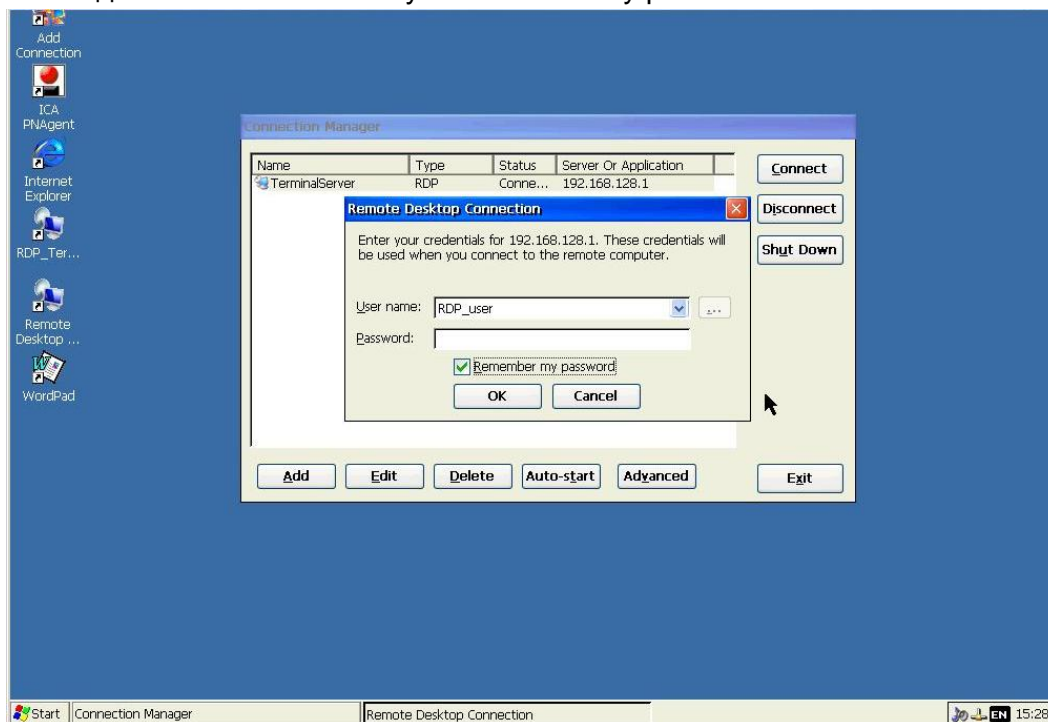
7. В окне Connection Manager и на рабочем столе появилось созданное подключение.



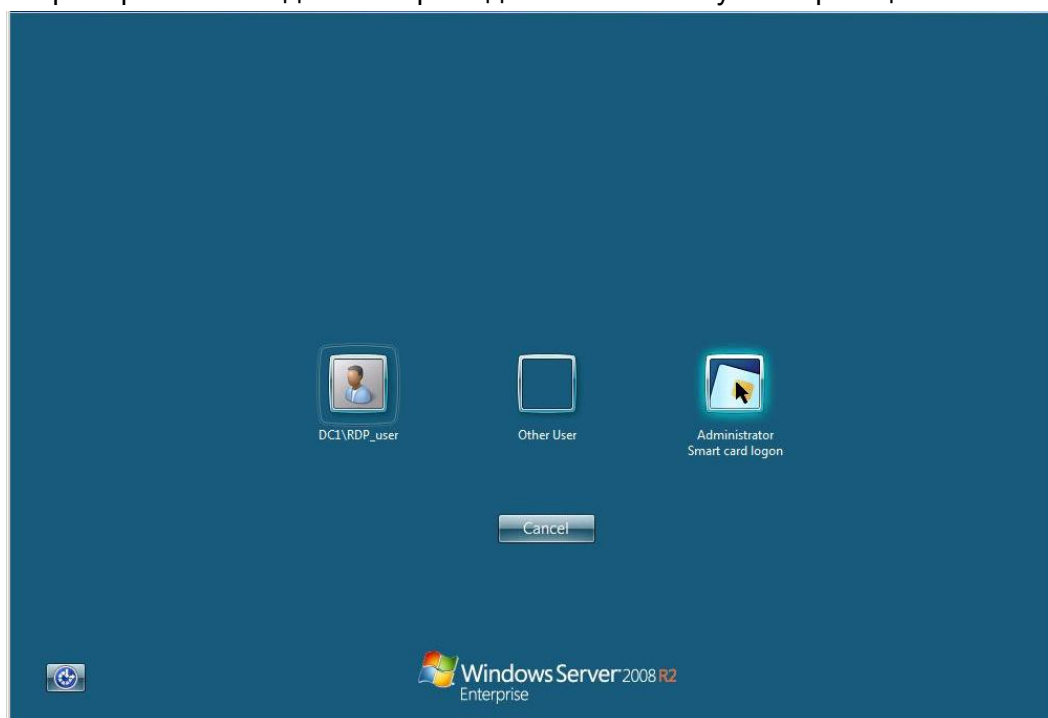
8. Подключить ключ eToken Pro Java с сертификатом пользователя к тонкому клиенту. **Подключать eToken к тонкому клиенту необходимо до установления терминальной сессии.**
9. Выбрать это подключение и нажать кнопку Connect.



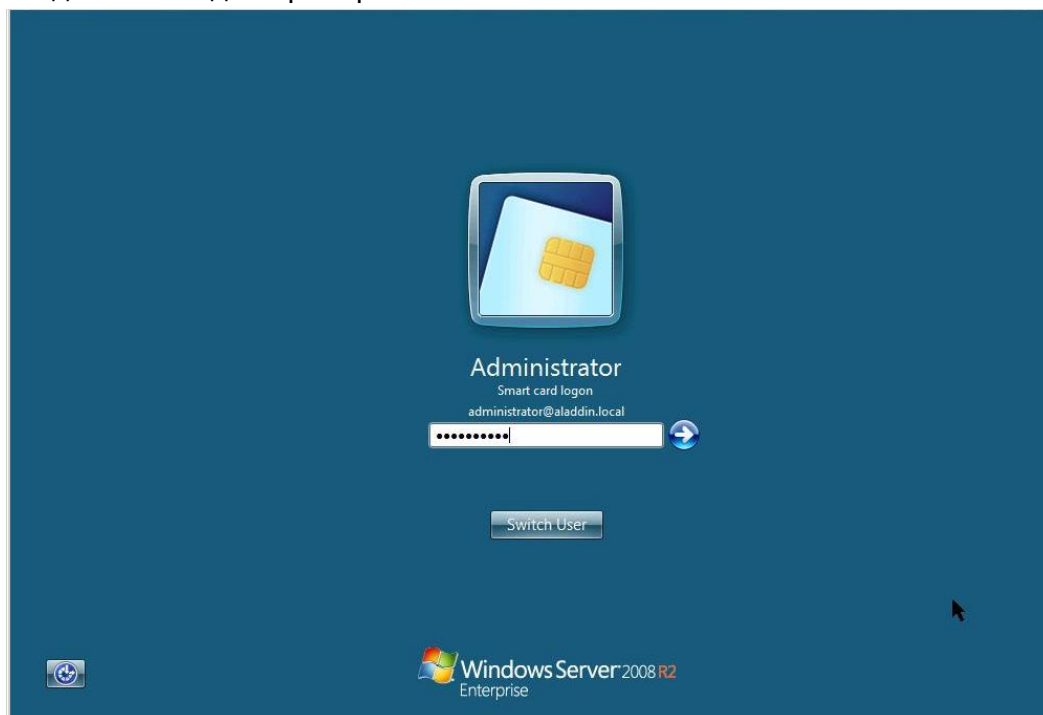
10. Ввести имя пользователя в поле User Name, поле пароль оставить пустым. Так же необходимо включить отметку «Remember my password». Нажать ОК.



11. Подключившись к терминальной сессии, Вы увидите вариант аутентификации по смарт-карте. Необходимо выбрать данный способ аутентификации.



12. Введите пин-код смарт-карты и нажмите Enter.



13. Осуществляется вход в терминальную сессию.

В дальнейшем, подключение к терминальному серверу с использованием аппаратных средств аутентификации возможно как с использованием ярлыка рабочего стола, так и менеджера терминальных соединений.

Автор настоящей инструкции:

Роман Совалов,

менеджер по работе с партнерами Aladdin Software Security R.D.

E-mail: dealer@aladdin.ru

Тел. +7(495)223-0001