3.1.3.5. Настройка подключения к терминальному серверу по предъявлению токена

Раздел содержит инструкцию по настройке подключения к терминалу по предъявлению токена.

Для настройки необходим компьютер с установленной операционной системой Windows 2019 Server Rus и драйверами Рутокен.

Операционная система должна быть настроена как **Контроллер домена**. В системе должны быть установлены и настроены **Службы сертификации** и **Службы терминалов (Службы удаленных рабочих столов**), а пользователям выданы сертификаты типа **Пользователь со смарт**картой или **Вход со смарт-картой**.

Все описанные далее действия производятся с административными правами в системе.

Для примера используется учетная запись Admin.

Этапы настройки подключения к терминальному серверу по предъявлению токена:

1 этап: Настройка Сервера терминалов.

2 этап: Настройка политик безопасности контроллера домена.

Настройка Сервера терминалов

Необходимо установить на сервере роль Службы удаленных рабочих столов (RDP) со службой Узел сеансов удаленных рабочих столов.

Если сервер является контроллером домена, то не рекомендуется устанавливать службу Посредник подключений к удаленному рабочему столу.

Для настройки Сервера терминалов:

- 1. Нажмите комбинацию клавиш Windows+X и выберите пункт меню Система.
- 2. В левой части окна Система щелкните по ссылке Настройка удаленного доступа.

🖳 Система				- 🗆 ×
🗧 🔶 🕤 🛧 🛃 > Панель уп	равления > Система и безопас	ность > Система	ٽ ~	Поиск в панели управления 🔎
Панель управления — домашняя страница	Просмотр основных с	зедений о вашем компьютере		
💡 Диспетчер устройств	Выпуск Windows			
Настройка удаленного	Windows Server 2016 Data	center		
доступа Дополнительные параметры	© Корпорация Майкросс	фт (Microsoft Corporation), 2016. Все права защищены.	, W	/indows Server [®] 2016
системы	Система			
	Процессор:	Intel(R) Core(TM) i5-6600 CPU @ 3.30GHz 3.31 GHz		
	Установленная память (ОЗУ):	4,00 ГБ		
	Тип системы:	64-разрядная операционная система, процессор х64		
	Перо и сенсорный ввод:	Перо и сенсорный ввод недоступны для этого экрана		
	Имя компьютера, имя домен	а и параметры рабочей группы		
	Имя компьютера:	WIN-1S5CABOT9FD		Изменить
	Полное имя:	WIN-1S5CABOT9FD.test.local		параметры
	Описание:			
	Домен:	test.local		
	Активация Windows			
	Система Windows не акти	вирована. Условия лицензионного соглашения на использ Майкрософт	ование програ	ммного обеспечения корпорации
	Код продукта: 00377-9000	0-00001-AA473		Активация Windows
См. также				
Центр безопасности и обслуживания				

- 3. В окне свойств системы перейдите на вкладку Удаленный доступ.
- 4. Установите переключатель в положение Разрешить удаленные подключения к этому компьютеру.
- 5. Установить галочку Разрешить подключение только...

6. Нажмите Выбрать пользователей.

	Оборудование	Дополнительно	Удаленный доступ
Удаленный пом	ющник		
Разрешить п компьютеру	юдключения удал	енного помощни	ка к этому
			Дополнительно
Удаленный раб	очий стол		
Выберите вариа	ант и укажите, ко	му разрешено по	дключение.
0.0	ть удаленные под	ключения к этом	у компьютеру
О не разрешат			
 Разрешить у 	даленные подклы	очения к этому к	омпьютеру
 Разрешить у Разрешить у Разрешить работает на уровне 	даленные подклю ть подключения т удаленный рабоч сети (рекоменду	очения к этому к олько с компьют ий стол с провер уется)	омпьютеру еров, на которых кой подлинности

При необходимости разрешить доступ к удаленным рабочим столам с компьютеров, не входящих в домен, или с компьютеров домена, работающих под управлением Windows XP, необходимо снять галочку с пункта **Разрешить подключения только с компьютеров, на** которых работает удаленный рабочий стол с проверкой подлинности на уровне сети (рекомендуется).

ользователи удаленного рабочего стола	?	×
ользователи из списка ниже, а также члены груп дминистраторы", могут подключаться к этому ко	пы мпьютеру.	
ST\Администратор уже имеет доступ.		
ругие группы, откройте панель управления <u>Учетны</u> ользователей.	ые записи	Телеи в
OK	Отм	ена
	ли группы поль	зователей, кото
ле Введите имена выбираемых объектов введите имя пользователя и уп к удаленным рабочим столам.		

"Пользователи" или "Группы"	Типы объектов
следующем месте:	
est.local	Размещение
ведите имена выбираемых объектов (п	римеры):
ведите <u>и</u> мена выбираемых объектов (<u>п</u> user1	римеры): Проверить имена
ведите <u>и</u> мена выбираемых объектов (<u>п</u> user1	<u>римеры):</u> Проверить имена

- 9. Нажмите Проверить имена.
- 10. Нажмите ОК.
- 11. Таким же образом добавьте других пользователей группы.

Настройка политик безопасности контроллеров домена

Для настройки политик безопасности контроллеров домена:

- 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 Управление групповой политикой.

🎕 🛃 📕 = I		Средства работы с ярлыками	Средства работы	с приложениями	Администрирование	- 0	×
Файл Главная	Поделиться Вид	Управление	Управ	ление			~ 🕐
← → · < 檔,	Панель управления >	Система и безопасность >	Администрирован	ие >	ٽ ~	Поиск: Администрирование	Q
🖈 Быстрый доступ	Имя ва_тиаршругиза Модуль Activ	^ ция и удаленный доступ re Directory для Windows P	Дата изменения 10.07.2010 10:19 16.07.2016 16:19	Тип лрлык Ярлык	Размер 2 кр 2 КБ		^
 Загрузки Документы Изображения 	 Монитор рес Оптимизация Очистка дися Пакет админ 	урсов я дисков ка истрирования диспетчера	16.07.2016 16:18 16.07.2016 16:18 16.07.2016 16:19 16.07.2016 16:19	Ярлык Ярлык Ярлык Ярлык	2 КБ 2 КБ 2 КБ 2 КБ		
System32	😥 Планировщи 🌄 Пользовател 🎦 Просмотр со	ик заданий и и компьютеры Active Dir обытий	16.07.2016 16:18 16.07.2016 16:20 16.07.2016 16:18	Ярлык Ярлык Ярлык	2 КБ 2 КБ 2 КБ		ł
💣 Сеть	📝 Редактирова 👰 Сведения о с 彛 Сервер поли	ние ADSI истеме тики сети	16.07.2016 16:19 16.07.2016 16:19 16.07.2016 16:20	Ярлык Ярлык Ярлык	2 КБ 2 КБ 2 КБ		
	🎲 Система архі 🔊 Системный і 🌮 Службы Місі	ивации данных Windows S ионитор rosoft Azure	16.07.2016 16:20 16.07.2016 16:18 16.07.2016 16:19	Ярлык Ярлык Ярлык	2 КБ 2 КБ 2 КБ		
1	🏞 Службы ком 🎊 Службы ᇌ Средство про	понентов оверки памяти Windows	16.07.2016 16:18 16.07.2016 16:18 16.07.2016 16:19	Ярлык Ярлык Ярлык	2 КБ 2 КБ 2 КБ		
	🛃 Управление і	групповой политикой	16.07.2016 16:19	Ярлык	2 КБ		
	Управление и Управление и Управление у Управление у Пенто замине у Пенто замине у В Пенто замине у В Пенто замине и В Пенто за в В Пенто за в В Пенто за в В Пенто и В Пенто в В Пенто и В Пенто за в В Пенто и В Пенто и В Пенто в В Пенто и В Пенто и И Пент	компьютером печатью удаленным доступом пистокрования Active Direc	16.07.2016 16:18 16.07.2016 16:19 16.07.2016 16:20 16.07.2016 16:19	Ярлык Ярлык Ярлык Ярлык	2 K6 2 K6 2 K6 2 K6		
Элементов: 36 Выб	дан Центр админ Бар Центр сертис ран 1 элемент: 1,19 КБ	инстрирования Астіче Direc фикации	16.07.2016 16:19	Ярлык	2 KB 2 K5		

В левой части окна Управление групповой политикой рядом с пунктом Объекты групповой политики щелкните по стрелочке.
 Щелкните правой кнопкой мыши по названию подпункта Default Domain Controllers Policy и выберите пункт Изменить...

🚠 Управление групповой политикой 🏽 Файл Действие Вид Окно Сі	равка			- U	× - 5
	•				
🕻 Управление групповой политикой	Default Domain C	ontrollers	Policy		
 ▲ Лес: test.local ◄ Домены 	Область Сведения Связи	Параметры	Делегирование	Состояние	
 Default Domain Policy Domain Controllers 	Показать связи в рас С GPO связаны следу	положении:	test.local омены и подраз	деления:	2
V 📑 Объекты групповой по	итики rollers Policy Размещение	^	Πρ	оинудительный	Св
 > Фильтры WMI > Ш Начальные объекть > Ш Сайты Ж Моделирование группово Результаты групповой пол 	Состояние объекта групповой поли Архивировать Восстановить из архива Импорт параметров	ітики >)й политики при мпьютеров:	именяются только	для
	Сохранить отчет Вид Новое окно отсюда	>			
	Копировать Удалить		C	войства	
	Обновить		ильтром WMI:	~ Откры	ІТЪ
	Справка				

7. В левой части окна Редактор управления групповыми политиками рядом с пунктом Конфигурация компьютера щелкните по стрелочке.

8. Рядом с пунктом Политики щелкните по стрелочке.

- 9. Рядом с пунктом Конфигурации Windows щелкните по стрелочке.
- 10. Рядом с пунктом Параметры безопасности щелкните по стрелочке.
- 11. Рядом с пунктом Локальные политики щелкните по стрелочке.
- 12. Щелкните по названию подпункта Назначение прав пользователя.

13. Два раза щелкните по названию политики Разрешить вход в систему через службу удаленных рабочих станций.

 Конфигурация компьютера Конфигурация программ Конфигурация программ Конфигурация Windows Политика разрешения имен Сценарии (запуск/завершение) Развернутые принтеры Параметры безопасности Политики учетных записей Политики зудита Политика аудита Параметры безопасности Драметры безопасности Курнал событий Системные службы Ресстр Файловая система Политики проводной сети (IEEE 802.: Брандмауэр Windows в режиме повы Политики открытого ключа Политики отраниченного использования 	 Политика Изменение параметров среды изготовителя Изменение системного времени Изменение часового пояса Имитация клиента после проверки подлинности Локальный вход в систему Настройка квот памяти для процесса Обход перекрестной проверки Отказать в доступе к этому компьютеру из сети Отказать в ов ходе в качестве пакетного задания Отказать во входе в качестве пакетного узла Отказать во входе в качестве службы Отключение компьютера от стиковочного узла Отладка программ Получить маркер олицетворения для другого пользоват Принудительное удаленное завершение работы Профилирование одного процесса Профилирование перационной системы Разрешение доверия к учетным записям компьютеров и Разрешение доверия к службы каталогов Синхронизация данных службы каталогов Смена владельцев файлов и других объектов 	Параметр г Администр Операторы Не определ КОНТРОЛЛ Администр Пред-Wind Не определ Не определ Не определ Администр Администр Не определ Администр Не определ Не определ Администр Не определ Администр Не определ Администр Не определ Администр Каминистр Не определ Администр Не определ			

14. Установите флажок Определить следующие параметры политики.

15. Нажмите Добавить пользователя или группу.

араметр политики безопасности	Объяснение		
Разрешить вход в систему столов	у через службу удаленн	ых рабочих	
Определить следующие параме	етры политики:		
Добавить пользователя или гру	ппу Удалить		
Данный параметр не совм Windows 2000 или более ра	естим с пакетом обнов анними версиями. Прим	вления 1 для меняйте	
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с бо операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена	вления 1 для иеняйте й параметр, Примен	ИТЪ
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с бо операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор.	вления 1 для иеняйте й параметр, Примен	ИТЪ
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией олее поздней версией мите Обзор. объектов введите имя поль Службы удаленных рабочих	вления 1 для иеняйте й параметр, Примен зователя или груп столов.	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией олее поздней версией мите Обзор. их объектов введите имя поль Службы удаленных рабочих о	вления 1 для иеняйте й параметр, и параметр, примен зователя или груп столов.	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией олее поздней версией объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб	вления 1 для иеняйте й параметр, и параметр, параметр, параметр, и параметр, и паратр, и параметр, и	ить ппы пользователей,
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с бо операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией олее поздней версией олее поздней версией отмена жмите Обзор. их объектов введите имя поль Службы удаленных рабочих , "Учетные записи служб	вления 1 для иеняйте й параметр, и параметр, параметр, параметр, и параметр, и паратр, и параметр, и	итъ
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с бо операционной системы. Не Добавление пользователя или группы наж не Выбор в поле Введите имена выбираемы вшено подключаться к этому серверу через мите Проверить имена. бор: "Пользователи", "Компьютеры", юберите тип объекта: Пользователи", "Учетные записи служб"	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией олее поздней версией объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб '. "Группы" или "Встрое	вления 1 для иеняйте й параметр, Примен зователя или груп столов. " или "Груп Типы объектов	ить пы пользователей, Х
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы. Не Добавление пользователя или группы наж не Выбор в поле Введите имена выбираемы зшено подключаться к этому серверу через иите Проверить имена. бор: "Пользователи", "Компьютеры", берите тип объекта: Іользователи", "Учетные записи служб" :ледующем месте:	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. их объектов введите имя поль Службы удаленных рабочих , "Учетные записи служб	вления 1 для иеняйте й параметр, и параметр, Примен зователя или груп столов. или "Груп Типы объектов	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы.	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. IX объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб	вления 1 для иеняйте й параметр, Примен зователя или груп столов. " или "Груп Типы объектов Размещение	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы. е Добавление пользователя или группы на- не Выбор в поле Введите имена выбираемых вшено подключаться к этому серверу через мите Проверить имена. бор: "Пользователи", "Компьютеры", берите тип объекта: loльзователи", "Учетные записи служб" следующем месте: st.local едите имена выбираемых объектов (при	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. IX объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб ', "Группы" или "Встрое	вления 1 для иеняйте й параметр, и параметр, Примен зователя или груп столов. или "Груп Типы объектов Размещение	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы. е Добавление пользователя или группы нах- е Выбор в поле Введите имена выбираемы зшено подключаться к этому серверу через- иите Проверить имена. бор: "Пользователи", "Компьютеры", берите тип объекта: Іользователи", "Учетные записи служб" ледующем месте: t.local едите <u>и</u> мена выбираемых объектов (при плание и совъектов (при	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. Ix объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб '. "Группы" или "Встрое	аления 1 для иеняйте й параметр, и параметр, Примен зователя или груп столов. " или "Груп Типы объектов Размещение Ъроверить имена	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы. е Добавление пользователя или группы нах е Выбор в поле Введите имена выбираемы ашено подключаться к этому серверу через ите Проверить имена. бор: "Пользователи", "Компьютеры", берите тип объекта: ользователи", "Учетные записи служб" ледующем месте: t.local эдите имена выбираемых объектов (при льзователи домена	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. IX объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб ', "Группы" или "Встрое	вления 1 для иеняйте й параметр, Примен зователя или груп столов. " или "Груп Типы объектов Размещение Ъроверить имена	ить
Данный параметр не совм Windows 2000 или более ра объекты групповой полити только к компьютерам с би операционной системы. е Добавление пользователя или группы нах- е Выбор в поле Введите имена выбираемы вшено подключаться к этому серверу через вите Проверить имена. бор: "Пользователи", "Компьютеры", берите тип объекта: Іользователи", "Учетные записи служб" педующем месте: t.local адите имена выбираемых объектов (при ользователи домена	естим с пакетом обнов анними версиями. Прим ки, содержащие данны олее поздней версией ОК Отмена жмите Обзор. IX объектов введите имя поль Службы удаленных рабочих о , "Учетные записи служб '. "Группы" или "Встрое	аления 1 для иеняйте й параметр, Примен зователя или груп столов. " или "Груп Типы объектов Размещение Ъроверить имена	ить

19. Нажмите ОК. В окне Добавление пользователя или группы отобразится имя пользователя или группы.

20. Нажмите **ОК**.

		ОК	Отмена	
ажмите ОК. Свойства: Разрешит	ь вход в систе	му через	службу уда	?
Параметр политики (безопасности	Объясне	ние	
Разрешить столов	вход в систем	у через слу	ужбу удаленны	х рабочих
Определить сле,	дующие парам	етры поли	тики:	
TEST\Пользовате	пи домена	202		
		197 S.		
	вателя или гру	/nny	Удалить	
Добавить пользо		естим с па	акетом обновл	ения 1 для еняйте
Добавить пользо Данный пар Windows 200 объекты гру только к ком	аметр не совм 10 или более ра пповой полити ипьютерам с б	анними ве іки, содерж олее позд	рсиями. Приме кащие данный ней версией	параметр,

22. Закройте окно оснастки Управление групповой политикой и окно Администрирование.

После перезагрузки компьютера настройка Служб удаленных рабочих столов и Политик безопасности контроллера домена будет завершена.

См. далее Настройка клиентской операционной системы.