2.1.3. Настройка входа в домен по предъявлению токена

Раздел содержит инструкцию по настройке входа в домен по предъявлению токена в операционной системе Windows Server 2019.

Для настройки необходим компьютер с установленной операционной системой Windows 2019 Server Rus и драйверами Рутокен, а также дистрибу тив этой OC.

Операционная система должна быть настроена как **Контроллер домена**, должны быть установлены **Службы Сертификации**, а пользователям выданы сертификаты типа **Пользователь со смарт-картой** или **Вход со смарт-картой**.

Все описанные действия производятся с правами администратора системы.

Для примера используется учетная запись Admin.

Этапы настройки входа в домен по предъявлению токена:

1 этап: Настройка учетных записей пользователя.

2 этап: Настройка политик безопасности домена.

3 этап: Настройка клиентской операционной системы.

Настройка учетных записей пользователей

В первую очередь необходимо настроить учетные записи пользователей. В этом примере будет настроена учетная запись **User** — пользователь домена, включенные только в группу **Пользователи домена**.

Для настройки учетной записи пользователя:

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

😰 администрирование - Панель управления	—		\times
 · · · · · · · · · · · · · · · · · · ·	админи	істрирова	×
Администрирование			
Оскать "администрирование" в центре справки и подде	ржки Win	dows	

В домене под управлением Windows Server 2019 есть возможность одним действием запретить всем входить в домен без наличия устройства Рутокен с необходимым сертификатом (пользователь с учетной записью Administrator также не сможет войти в домен без наличия устройства Рутокен). Шаги 2-5 данной инструкции необходимо выполнить только в том случае, если в домене будут пользователи не только с устройствами Рутокен, но и использующие альтернативные способы аутентификации (пароли, биометрические данные и т. д.). При этом шаги 9-10 надо пропустить.

4. Два раза щелкните по названию Пользователи и компьютеры Active Directory.

айл Главная По	делиться Вид		×
→ ~ ↑ 🗟 « Ci	истема и безопасность 🚿 Администрирование	~ С Поиск	: Админ 🔎
	Лмя	Дата изменения	Тип
📌 Быстрый доступ	😫 Оптимизация дисков	16.07.2016 16:18	Ярлык
📃 Рабочий стол 🖈	🔚 Очистка диска	16.07.2016 16:19	Ярлык
🖊 Загрузки 🛛 🖈	💮 Планировщик заданий	16.07.2016 16:18	Ярлык
🟥 Документы 💉	📃 Пользователи и компьютеры Active Directory	16.07.2016 16:20	Ярлык
📰 Изображения 🖈	🔠 Просмотр событий	16.07.2016 16:18	Ярлык
System32	💦 Редактирование ADSI	16.07.2016 16:19	Ярлык
	👰 Сведения о системе	16.07.2016 16:19	Ярлык
💻 Этот компьютер	🎲 Система архивации данных Windows Server	16.07.2016 16:20	Ярлык
💣 Сеть	🔊 Системный монитор	16.07.2016 16:18	Ярлык

5. В левой части окна оснастки щелкните по названию папки Users.

6. Щелкните правой кнопкой мыши по имени пользователя, которому будет разрешено входить в домен только при наличии устройства Рутокен, и выберите пункт **Свойства**.

🔿 🙋 📷 🖌 📋 🗙 🛅 🙆	🛓 🛛 🖬 🗏 🔽 🛅 🔻	2 🐍		
Пользователи и компьютеры / > Сохраненные запросы > Etst.local > Вuiltin > Computers > © Domain Controllers	Admins SUpdateProxy androv tected Users	Тип Группа безоп Группа безоп Пользователь Группа безоп	Описание Группа администратор DNS-клиенты, которы Участникам этой групп	^
 ForeignSecurityPrincipal: Managed Service Accour Users Aan A	И Копировать иин Добавить в группу иин Отключить учетнук иин Отключить учетнук иин Смена пароля иин Переместить иин Открыть домашнюн открыть домашнюн отправить почту ть Все задачи ппа Вырезать удалить рниц Переименовать	о страницу	 троенная учетная за ззначенные админис тены этой группы мо тены этой группы мо ззначенные админис ззначенные админис ззначенные админис троенная учетная за троенная учетная за эроли членов данной тены этой группы мо тены этой группы мо 	
Кон	про		е контроллеры доме	

7. В окне свойств пользователя перейдите на вкладку Учетная запись.

8. В секции Параметры учетной записи установите флажок Для интерактивного входа в сеть нужна смарт-карта. Нажмите на кнопку [ОК].

Член груг	nn Bx	одящие звонки	Среда	Сеанс	ы	Удале	енное	е упр	авл	ение
Пр	офиль (служб удаленных	к рабочио	столов	8			CON	1+	
Общие	Адрес	Учетная запи	сь Про	филь	Ter	пефон	ы (Орга	низ	ация
Имя вхо	да пол	ьзователя:								
user1			@te	st.local					~	
Имя вхо	ола пол	ьзователя (прел	-Windows	2000).						
TEST			user	1						
Врем: Разб Параме	я входа і́локиро	Вход н вать учетную за атной записи:	на							
Врем. Разб Параме	я входа і́локиро тры уче ранить г	Вход н вать учетную за етной записи: пароль, использу	на пись уя обрать	імое ши	ιφро	вание	1		^	
Врем. Разб Параме Хр От Пара	я входа о́локиро тры уче ранить г тключит	Вход н вать учетную за етной записи: пароль, использу ъ учетную запис	на пись уя обрать ь	мое ши		вание			^	
Врем. Разб Параме Хр От Ду	я входа (локиро атры уче ранить г пключит пя инте нетная з	Вход н вать учетную за этной записи: пароль, использу ть учетную запис рактивного вход запись важна и н	на пись уя обрать ь а в сеть не может	имое ши нужна с быть д	іфро жар	вание т-карт гирова	га	3	• • • • • • • • • • • • • • • • • • •	1
Врем. Разб Параме Хр От От От	я входа і́локиро тры уче ранить г пключит пя инте нетная з	Вход н вать учетную за атной записи: пароль, использу ъ учетную запис рактивного вход запись важна и н	на пись уя обрать ь а в сеть не может	імое ши нужна с быть д	іфро :мар елег	вание т-карт ирова	а	3	< ×	1
Врем. Разб	я входа (локиро тры уче ранить г пя инте нетная з действи	Вход н вать учетную за атной записи: пароль, использу ъ учетную запис рактивного вход запись важна и н я учетной запис	на пись уя обрать а в сеть не может и	імое ши нужна с быть д	іфро смар елег	вание т-карт ирова	ана	1	×	1
Врем. Разб Параме Хр От Дл Срок л От	я входа опокиро пры уче ранить г пключит пя инте нетная з цействи икогда	Вход н вать учетную за етной записи: пароль, использу ъ учетную запис рактивного вход запись важна и н ия учетной запис	на пись уя обрать ь а в сеть не может и	имое ши нужна с быть д	іфро смар елег	вание т-карт ирова	а		^	1

- 9. Закрой окно Active Directory пользователи и компьютеры.
- **10.** Аналогичным образом настройте другие учетные записи в домене. Для таких пользователей вход в домен будет доступен только при наличии устройства Рутокен с сертификатом, выданным администратором домена.

Настройка политик безопасности домена

Для настройки политик безопасности:

- 1. Откройте Панель управления.
- 2. Два раза щелкните по названию пункта Администрирование.

3. Два раза щелкните по названию оснастки Управление групповой политикой.

грирование Средства работы с ярлыками			
елиться Вид Управление		~ (0
стема и безопасность 🔸 Администрирование	∨ О Поиск	Админ 🔎	
Ами	Дата изменения	Тип	^
🌮 Службы Microsoft Azure	16.07.2016 16:19	Ярлык	
🌮 Службы компонентов	16.07.2016 16:18	Ярлык	
🖂 Службы	16.07.2016 16:18	Ярлык	
👔 Средство проверки памяти Windows	16.07.2016 16:19	Ярлык	
😹 Управление групповой политикой	16.07.2016 16:19	Ярлык	
🎥 Управление компьютером	16.07.2016 16:18	Ярлык	
汩 Управление печатью	16.07.2016 16:19	Ярлык	
📑 Центр администрирования Active Directory	16.07.2016 16:19	Ярлык	
🚋 Центр сертификации	16.07.2016 16:19	Ярлык	¥
<		>	
	трирование Средства работы с ярлыками целиться Вид Управление истема и безопасность > Администрирование Имя Олужбы Microsoft Azure Службы компонентов Службы компонентов Службы компонентов Службы Средство проверки памяти Windows Управление групповой политикой Управление групповой политикой Управление печатью Центр администрирования Active Directory Центр сертификации	трирование Средства работы с ярлыками — целиться Вид Управление Стема и безопасность > Администрирование Стема и безопасность > Администрирование Службы Місгозоft Azure 16.07.2016 16:19 Службы компонентов 16.07.2016 16:18 Службы 16.07.2016 16:18 Службы 16.07.2016 16:18 Средство проверки памяти Windows 16.07.2016 16:19 Службы 16.07.2016 16:19 Управление групповой политикой 16.07.2016 16:19 Управление печатью 16.07.2016 16:19 Управление печатью 16.07.2016 16:19 Центр администрирования Active Directory 16.07.2016 16:19 Центр сертификации 16.07.2016 16:19	трирование Средства работы с ярлыками – С Х целиться Вид Управление V C Поиск: Администрирование V C Поиск: Админ Р Имя Дата изменения Тип Службы Microsoft Azure 16.07.2016 16:19 Ярлык Службы компонентов 16.07.2016 16:18 Ярлык Службы 16.07.2016 16:18 Ярлык Службы 16.07.2016 16:19 Ярлык Средство проверки памяти Windows 16.07.2016 16:19 Ярлык Средство проверки памяти Windows 16.07.2016 16:19 Ярлык Управление групповой политикой 16.07.2016 16:19 Ярлык Управление печатью 16.07.2016 16:19 Ярлык Управление печатью 16.07.2016 16:19 Ярлык Управление печатью 16.07.2016 16:19 Ярлык Службы 16.07.2016 16:19 Ярлык Службы 16.07.2016 16:19 Ярлык Средство проверки памяти Windows 16.07.2016 16:19 Ярлык С управление печатью 16.07.2016 16:19 Ярлык С управление печатью 16.07.2016 16:19 Ярлык Центр администрирования Active Directory 16.07.2016 16:19 Ярлык Центр сертификации 16.07.2016 16:19 Ярлык

- 4. В окне Управление групповой политикой рядом с названием категории Объекты групповой политики щелкните по стрелочке.
- 5. Щелкните правой кнопкой мыши по названию объекта групповой политики Default Domain Policy и выберите пункт Изменить...

🐤 🔿 🖄 📰 🖏 🗐 🗙 🝳 🛙	Default Domain Controll	are Policy
 A Лес: test.local ✓ Домены ✓ щ test.local ✓ щ test.local ✓ ш test.local ✓ ш Default Domain Policy > ם Domain Controllers 	Область Сведения Парамет Связи Показать связи в расположени С GPO связаны следующие сай	н Белегирование Состояние и: test.local ты, домены и подразделения:
 Объекты групповой по Default Domain Con Default Domain Фильтры WMI Пачарыные объекть 	литики trollers Policy Изменить Состояние объекта групповой политики	Принудительный Св Нет Да
Райты В Моделирование группово Результаты групповой пол В Результаты групповой пол	Архивировать Восстановить из архива Импорт параметров Сохранить отчет Вид Новое окно отсюда	ий политики применяются только для мпьютеров:
	Копировать	Свойства

Шаги 4-5 необходимо выполнять только в том случае, если всем пользователям будет запрещен вход в домен без устройства Рутокен с необходимым сертификатом.

- 6. В окне Редактор управления групповыми политиками рядом с названием пункта Конфигурация Windows щелкните по стрелочке.
- 7. Рядом с названием пункта Параметры безопасности щелкните по стрелочке.
- 8. Рядом с названием пункта Локальные политики щелкните по стрелочке.
- 9. Щелкните по названию пункта Параметры безопасности.

10. Щелкните два раза по названию политики Интерактивный вход в систему: требовать Windows Hello для бизнеса или смарт- карту.

11. Установите флажок Определить следующий параметр политики.

12. Установите переключатель в положение Включен.

13. Нажмите на кнопку [ОК].

биства: интерактивный вход в	систему: требовать с	?	×
араметр политики безопасности	Объяснение		
Интерактивный вход в си	стему: требовать смарт-ка	рту	
Определить следующий пара	метр политики:		
Включен			
Отключен			
F	ОК Отмена	Поне	

14. В окне Редактор управления групповыми политиками рядом с пунктом Конфигурации Windows щелкните по стрелочке.

15. Рядом с названием подпункта Параметры безопасности щелкните по стрелочке.

16. Рядом с названием Локальные политики щелкните по стрелочке.

17. Щелкните по названию подпункта Параметры безопасности.

 Щелкните правой кнопкой мыши по названию политики Интерактивный вход в систему: поведение при извлечении смарт-карты и выберите пункт Свойства.



19. Установите флажок Определить следующий параметр политики.

20. Из раскрывающегося списка выберите поведение клиентской ОС при отсоединении устройства Рутокен в процессе открытого пользовательского сеанса. В данном примере выбрано поведение ОС — **Блокировка рабочей станции**.

21. Нажмите на кнопку [ОК].



22. Закройте окно Редактор управления групповыми политиками.

23. Закройте Панель управления.

Настройка будет доступна только после перезагрузки компьютера. Настройка серверной операционной системы после этого будет завершена.

Настройка клиентской операционной системы

Компьютеры с установленными клиентскими операционными системами Windows 10/8.1/8/7/Vista/XP/2000 необходимо ввести в домен и установить на них драйверы Рутокен.

Редакции ОС должны включать возможность присоединения к домену.

Если клиентские компьютеры были загружены во время настройки сервера, то необходимо их перезагрузить.

Теперь пользователи, которым выдан сертификат типа **Пользователь со смарт-картой** или **Вход со смарт-картой**, смогут входить в домен только при подключении к компьютеру устройства Рутокен с этим сертификатом.

При извлечении устройства Рутокен в процессе открытого пользовательского сеанса, клиентская ОС будет автоматически заблокирована (в ОС Windows 10/8.1/8/7/Vista для блокировки рабочего стола при отключении устройства Рутокен необходимо установить автоматический запуск службы Политика удаления смарт-карт/Smart Card Removal Policy).