3.1.3.2. 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	_		×
 · · · · · · · · · · · · · · · · · · ·	админи	стрирова	×
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 устойства 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**.

Þ 🔿 📊 🔏 📋 🗙 🛅	a 🗟 🛛 🖬 🖏 🐮	7 🗾 🐍		
 Пользователи и компьютеры /	мя DnsAdmins DnsUpdateProxy Nikandrov Protected Users	Тип Группа безоп Группа безоп Пользователь Группа безоп	Описание Группа администратор DNS-клиенты, которы Участникам этой групп	^
 ForeignSecurityPrincipal: Managed Service Accounting Users 	узегі і Админ Добавить в груп Админ Добавить в груп Админ Отключить учет Админ Смена пароля Админ Переместить Админ Открыть домаш Владел Отправить почт Гости д Гости д Госта Все задачи Группа Вырезать Удалить Клони; Переименовать	пу тную запись инюю страницу у	троенная учетная за ззначенные админис тены этой группы мо тены этой группы мо ззначенные админис ззначенные админис тены этой группы мо те гости домена троенная учетная за зроли членов данной тены этой группы мо тены этой группы мо	
	Компы Свойства Контрс		е рабочие станции и 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 ОК.

Член гру	ynn B	ходя	ящие звонки	Среда	Сеано	сы	Удал	енно	е упр	авл	ение
Πρ	офиль	слу	жб удаленных	к рабочио	столов	3			COI	vl+	
Общие	Адре	C I	Учетная запи	сь Про	филь	Te	лефон	ы	Орга	низ	ация
Имя вх	ода по	пьзо	вателя:								
user1				@te	st.local					~	
Имя вх	ола по	1630	вателя (пред	-Windows	2000).						l
TEST				use	1						
Bpen Pas Napame	ия вход блокир етры уч	а ова етн	Входн ть учетную за ой записи:	на							
Bpen Pase Napame	ия вход блокир етры уч ранить	а ова етно пар	Входн ть учетную за ой записи: оль, использу	на пись уя обрать	мое ши	ифро	ование	•		^	
Bpen Pas Napame	ия вход блокир етры уч ранить тключи	а ова пар	Входн ть учетную за ой записи: оль, использу четную запис	на пись уя обрать ь	мое ши		рвание)		^	
	ия вход блокир етры уч ранить тключи Іля инт учетная	а ова етни пар тъ у ерак зап	Входн ть учетную за ой записи: оль, использу четную запис тивного вход ись важна и н	на пись уя обрать ь а в сеть не может	имое ши нужна с быть д	ифро	ование от-карт	; ra aHa		^	1
	ия вход блокир етры уч ранить тключи (ля инт учетная	а ова етни пар тъ у ерак зап	Вход н ть учетную зап ой записи: оль, использу четную запис тивного вход ись важна и н	на пись уя обрать ь а в сеть не может	имое ши нужна с быть д	ифро смар	ование от-карт гирова	; ra зна	2	*	1
	ия вход блокир етры уч ранить тключи (ля инто учетная действ	а ова пар пъ у ерак зап	Вход н ть учетную зап ой записи: оль, использу четную запис стивного вход ись важна и н четной запис	на пись уя обрать ь а в сеть не может и	имое ши нужна с быть д	ифро смар	ование от-карт гирова	; та эна	2	^ >	1
Врем Раз Парами Срок О Срок О Н	ия вход блокир етры уч ранить тключи (ля инт- икогда икогда	а ова пар пъ у ерак зап	Вход н ть учетную зап ой записи: оль, использу четную запис тивного вход ись важна и н четной запис	на пись уя обрать ь а в сеть не может и	імое ши нужна с быть д	ифро смар	ование от-карт гирова	та	3	^	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.

😤 🎴 🔚 🖛 Админич	стрирование Средства работы с ярлыками	-	
Файл Главная По	делиться Вид Управление		~ (
← → ∽ ♠ « C	истема и безопасность 🔸 Администрирование	∨ С Поиск	Админ 🔎
	Имя	Дата изменения	Тип
📌 Быстрый доступ	Службы Microsoft Azure	16.07.2016 16:19	Ярлык
Рабочии стол 🚿	訡 Службы компонентов	16.07.2016 16:18	Ярлык
🕂 Загрузки 🛛 🖈	🍰 Службы	16.07.2016 16:18	Ярлык
🟥 Документы 🛛 🖈	🏽 Средство проверки памяти Windows	16.07.2016 16:19	Ярлык
📰 Изображения 🖈	🛃 Управление групповой политикой	16.07.2016 16:19	Ярлык
System32	🌆 Управление компьютером	16.07.2016 16:18	Ярлык
	🔚 Управление печатью	16.07.2016 16:19	Ярлык
💻 Этот компьютер	🛃 Центр администрирования Active Directory	16.07.2016 16:19	Ярлык
💣 Сеть	🚋 Центр сертификации	16.07.2016 16:19	Ярлык
	<		>
Элементов: 31 Выбран	і 1 элемент: 1,13 KБ		

- 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...



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.

• 🔿 📶 🗙 🖫 🗟 🔢 🖬
Конфигурация компьютера Конфигурация программ Конфигурация программ Конфигурация программ Конфигурация программ Конфигурация плограмм Конфигурация плограмм Конфигурация плограмм Политика разрешения имен Политика разрешения имен Политика разрешения имен Политика разрешения Политика аудита Политика аудита Политика аудита Политика аудита Политика аудита Политика аудита Политика аудита Политика аудита Конфигурация пользователя Политика аудита Сстемные службы Событий Событий Политика испетчера списка сетей Политика испетчера списка сетей Собъюто и поравления приложения Политика испетчера списка сетей Собъюто и поравления приложения Собъюто и поравления приложения Политика испетчера списка сетей Политика истератого клоча Политика истератого клоча Политика истератого клоча Политика истератого клоча Политика истраниченного использо Политика истараниченного использо Адиминстративные шаблоных получены о Настройка

11. Установите флажок Определить следующий параметр политики.

12. Установите переключатель в положение Включен.

13. Нажмите **ОК**.

Свойства: Интерактивный вход в о	систему: требовать с	?	×
Параметр политики безопасности	Объяснение		
Интерактивный вход в сис	тему: требовать смарт-кар	ту	
Определить следующий парам	етр политики:		
Включен			
Отключен			
	ОК Отмена	Прим	енить

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 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).