3.1.4.2. Настройка входа в домен по предъявлению токена

Раздел содержит инструкцию по настройке входа в домен по предъявлению токена в операционной системе Windows Server 2022.

Для настройки необходимы:

- компьютер с установленной операционной системой Windows 2022 Server Rus;
- установленные Драйверы Рутокен;
- дистрибутив ОС.

Необходимые условия:

- операционная система настроена как Контроллер домена;
- установлены Службы Сертификации;
- 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.

Если необходимо настроить учетную запись для конкретного пользователя, то выполните процедуру, описанную в разделе.

Если необходимо выполнить настройку для группы пользователей, то выполните процедуру, описанную в разделе.

Для настройки клиентской ОС, выполните процедуру, описанную в разделе.

Настройка учетной записи пользователя

В первую очередь необходимо настроить учетные записи пользователей.

В этом примере будет настроена учетная запись User — пользователь домена, который включен только в группу Пользователи домена.

Для настройки учетной записи пользователя:

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



4. Два раза щелкните Пользователи и компьютеры Active Directory.

айл Главная Г	оделиться Вид		~
→ · ↑ 🗟 «	Система и безопасность > Администрирование	🗸 🖸 Поиск	: Админ 🔎
	Имя	Дата изменения	Тип
📌 Быстрый доступ	ڬ 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 папке Users.

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

Файл Действие Вид Справка			
	1 🖬 🕺 📚 🗃 🍸 🖉 🗞	0	
> Сохраненные запросы > Сохраненные запросы > Вuiltin > Computers © Domain Controllers > Domain Controllers	dmins Группа безоп pdateProxy Группа безоп ndrov Пользователь cted Users Группа безоп	Описание Группа администратор DNS-клиенты, которы Участникам этой групп	
 ForeignSecurityPrincipal: Managed Service Accour Managed Service Accour Адми Адми	Копировать н Добавить в группу н Отключить учетную запись н Смена пароля Переместить Открыть домашнюю страницу отправить почту Все задачи вырезать удалить и Переименовать	троенная учетная за ззначенные админис тены этой группы мо ззначенные админис ззначенные админис значенные админис тены этой группы мо се гости домена троенная учетная за зроли членов данной зроли членов данной тены этой группы мо тены этой группы мо	
<u> Конт</u>		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.

Профиль служб удаленных рабочих столов СОМ+ Общие Адрес Учетная запись Профиль Телефоны Организация Имя входа пользователя: user1 @test.local // Имя входа пользователя (пред-Windows 2000): TEST\ user1 Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована / Срок действия учетной записи () Истекает: 2 марта 2023 г.	Член гру	nn	Bxog	ящие зв	онки	Среда	Сеано	сы	Уда	ленн	юе уп	равл	ение
Общие Адрес Учетная запись Профиль Телефоны Организация Имя входа пользователя: user1 @test.local Имя входа пользователя (пред-Windows 2000): TEST\ Bpeмя входа Вход на Pasблокировать учетную запись Параметры учетной записи: Xpaнить пароль, используя обратимое шифрование Oтключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Otkлючить учетной записи Yuethaя запись важна и не может быть делегирована Vuethaя учетной записи Mukorga Utrekaet: 2 марта 2023 г.	Πŗ	рофил	ь сл	ужб удал	тенных	рабочих	СТОЛОВ	3			CO	M+	
Имя входа пользователя: шser1 @test.local Имя входа пользователя (пред-Windows 2000): TEST\ user1 Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никогда Истекает: 2 марта 2023 г.	Общие	Адр	ec	учетна	я запис	ь Про	филь	Te	лефа	оны	Орг	аниз	зация
user1 @test.local Имя входа пользователя (пред-Windows 2000): TEST\ user1 Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Учетная запись важна и не может быть делегирована Отключить учетной записи Никогда Истекает: 2 марта 2023 г.	Имя вх	ода п	ольз	ователя	:								
Имя входа пользователя (пред-Windows 2000): TEST\ user1 Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никогда Истекает: 2 марта 2023 г.	user1					@te	st.local					~	
ТЕЗТ\ user1 Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никог да Истекает: 2 марта 2023 г.	Имя вх	ода п	ольз	ователя	(пред-V	Nindows	2000):						
Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Учетная запись важна и не может быть делегирована Срок действия учетной записи Ю Никогда Истекает: 2 марта 2023 г.	TEST				11-4	user	1						1
Время входа Вход на Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Учетная учетной записи Рикогда Истекает: 2 марта 2023 г.	1.0000											- 9	1
 Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никог да Истекает: 2 марта 2023 г. 													
 Разблокировать учетную запись Параметры учетной записи: Хранить пароль, используя обратимое шифрование Отключить учетную запись Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никогда Истекает: 2 марта 2023 г. 	Врем	ия вхо	да		Вход на	a							
 Для интерактивного входа в сеть нужна смарт-карта Учетная запись важна и не может быть делегирована Срок действия учетной записи Никогда Истекает: 2 марта 2023 г. 	Врем	ия вхо блоки	да	ать учетн	Вход на кую запі	а							
 Учетная запись важна и не может быть делегирована Срок действия учетной записи Никогда Истекает: 2 марта 2023 г. 	Bpen Pas Napame	ия вхо блоки етры у ранит	рова учетн ъ па	ать учетной запи	Вход на кую запи си: пользуя	а ись я обрати	мое ши	ифро	рвани	ие		^	
Срок действия учетной записи • Никогда • Истекает: 2 марта 2023 г.	Bpen Pass Napame	ия вхо блоки етры у ранит тключ	рова учетн ъ пар нитъ	ать учетн юй запи роль, ис учетную ктивног	Вход на ную запи си: пользуя запись	а ись я обрати	имое ши	ифро	рвани	ие	-	^	
Срок действия учетной записи • Никогда Истекает: 2 марта 2023 г.		ия вхо блоки етры у ранит тключ Іля ин	рова учетн ъ пај чить тера	ать учетн юй запи роль, ис учетную ктивног	Вход на ную запи си: пользуя запись о входа кна и не	а ись я обрати в сеть е может	имое ши нужна с быть д	смар	овані от-ка	ие рта вана	-	• • • •	1
 Никогда Истекает: 2 марта 2023 г. 		ия вхо блоки етры у ранит тключ Іля ин учетна	рова учетн ъ па нить тера я за	ать учетн юй запи роль, ис учетную ктивног пись вах	Вход на кую запи си: пользуя запись о входа кна и не	а ись я обрати в сеть е может	имое ши нужна с быть д	ифро смар	овані от-ка гиро	ие рта вана	-	*	1
ОИстекает: 2 марта 2023 г	Врем Раз Парами Х О О У У	ия вхо блоки етры у ранит тключ Іля ин учетна дейст	да рова учетн ъ па нить тера я за	ать учетн юй запи роль, ис учетную ктивног пись вах учетной	Вход на ную запи си: пользуя запись о входа кна и не записи	а ись я обрати в сеть а может	імое ши нужна с быть д	ифро смар	рвани от-ка гиро	ие рта вана		•	1
	Врем Раз Парами Срок О Срок О Н	ия вхо блоки етры у ранит тключ Іля ин учетна дейст икогд	да рова учетн ъ па иить тера я за пвия ца	ать учетной запи ной запи роль, ис учетную ктивного пись вах учетной	Вход на ную запи си: пользуя запись о входа кна и не записи	а ись я обрати в сеть е может	имое ши нужна с быть д	ифро смар делеі	овани от-ка гиро	ие рта вана		* * *	1
	Врем Раз Парами Х О У Срок О И	ия вхо блоки етры у ранит тключ (ля ин дейст икогд Істека	да рова учетн ь па иить тера я за пвия ца ает:	ать учетн юй запи роль, ис учетную ктивног пись вах учетной	Вход на кую запи си: пользуя запись о входа кна и не записи 4арта	а ись а обрати в сеть а может 2023 г.	имое ши нужна с быть д	ифро смар	рвані рт-ка	ие рта вана			1

Настройка политик безопасности домена

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

Для настройки политик безопасности:

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

^{9.} Закройте окно Active Directory - пользователи и компьютеры.

3. Два раза щелкните по оснастке Управление групповой политикой.

📸 🛃 📕 🖛 Админис	трирование	Средства работы с ярлыками		÷.		×
Файл Главная Под	делиться Вид	Управление				1
← → × ↑ 🚟 « Cu	истема и безопасное	ть > Администрирование	✓ [™]	Поиск:	Админ	Q
	Имя	^	Дата изме	нения	Тип	^
🖈 Быстрый доступ	🜮 Службы Міс	rosoft Azure	16.07.2016	16:19	Ярлык	
📃 Рабочий стол 🖈	🌮 Службы ком	понентов	16.07.2016	16:18	Ярлык	
👆 Загрузки 🛛 🖈	🐊 Службы		16.07.2016	16:18	Ярлык	
🚆 Документы 🛛 🖈	🚛 Средство пр	оверки 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	-
	汩 Управление	печатью	16.07.2016	16:19	Ярлык	
💻 Этот компьютер	🛃 Центр админ	истрирования Active Directory	16.07.2016	16:19	Ярлык	
🔿 Сеть	🚋 Центр серти	фикации	16.07.2016	16:19	Ярлык	~
	<					>
Элементов: 31 Выбран	1 элемент: 1,13 КБ				=	-

4. В окне Управление групповой политикой нажмите на категорию Объекты групповой политики.

5. Щелкните правой кнопкой мыши по названию объекта групповой политики Default Domain Policy и выберите пункт Изменить...

Управление групповой политик Файл Лействие Вил Окно.	ой		— [
 Управление групповой политика Доке: Домены Домены Домены Домены Домены Домены Домены Объекты группово Ofъекты Группово Default Domain 	су й политики Controllers Policy	Default Domain Pc Область Сведения Связи Показать связи в раст С GPO связаны следуи Размещение Фазнецение Вайно по	оlicy Параметры // положении: а ощие сайты, до	Qenerv ()) aktiv.ru () омены и по,
> 🚔 Фильтры WMI > 🛅 Начальные объ	Изменить Состояние объекта групповой политики	>		>
 Парадини Сайты Моделирование группа Результаты групповой 	Архивировать Восстановить из архива Импорт параметров Сохранить отчет	ильтры безопасн раметры данного об едующих групп, поль імя	ости бъекта группов озователей и ко	юй политик омпьютеро
	Вид Новое окно отсюда	>	Прошедшие проверку	
Открытие редактора объектов гру	Копировать Удалить Переименовать Обновить	Добавить ильтр WMI 5ъект GPO связан с	Удалить о следующим о	э Фильтром W

6. В окне Редактор управления групповыми политиками нажмите на пункт Конфигурация Windows.

7. Нажмите на пункт Параметры безопасности.

8. Нажмите на пункт Локальные политики.

9. Нажмите на пункт Параметры безопасности.

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

Редактор управления групповыми политиками	- 0	ı X
Файл Действие Вид Справка		
🗸 👰 Конфигурация компьютера 🔨	Политика	Парамі ^
Политики	DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)	Не опр
> 🧮 Конфигурация программ	DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)	Не опр
🗸 🛄 Конфигурация Windows	а верти отраничения компаютера на запуск в силтакенсе вове (всеансу везспреот великон сандааде)	Не опр
> Политика разрешения имен	а лудит вудит доступа пловольных системных объектов	Неопр
🔄 Сценарии (запуск/завершение)	Одника издин использования привилстии на вримацию и восстановление	Hearp
> Развернутые принтеры	Од Аудит. немедленное отключение системы, если невозможно внести в журнал записи об аудите безопас	Hearp
Параметры безопасности	щі Аудит: принудительно переопределяєт параметры категории политики аудита параметрами подкатегор	Omena
> jjii Политики учетных записей	од доступ к сеги: Разрешить трансляцию анонимного зор в имя	
Локальные политики	щ завершение расоты: очистка фаила подкачки виртуальной памяти	не опр
> 🧾 Политика аудита	щі завершение работы: разрешить завершение работы системы без выполнения входа в систему	не опр
> 🚛 Назначение прав пользователя	Ш Интерактивный вход в систему: поведение при извлечений смарт-карты	Не опр
📑 Параметры безопасности	Ш Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему	Не опр
> Д Журнал событий	Ш Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия дост	Не опр
> I руппы с ограниченным доступом	Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	Не опр
> 🛕 Системные службы	Ш Интерактивный вход в систему: не отображать имя пользователя при входе в систему	Не опр
> Реестр	Ш Интерактивный вход в систему: не отображать учетные данные последнего пользователя	Не опр
> 🙀 Фаиловая система	🖏 Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Не опр
) Политики проводной сети (IEEE 802.)	📓 Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован.	Не опр
> Монитор брандмауэра Защитника \	💹 Интерактивный вход в систему: пороговое число неудачных попыток входа	Не опр
Политики диспетчера списка сетеи	💹 Интерактивный вход в систему: предел простоя компьютера	Не опр
> 🔐 Политики беспроводной сети (IEEE)	💹 Интерактивный вход в систему: текст сообщения для пользователей при входе в систему	Не опр
> Политики открытого ключа	Интерактивный вход в систему: требовать Windows Hello для бизнеса или смарт-карту	Не опр
Политики ограниченного использо	🔯 Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки ко	Не опр
Политики управления приложения	📓 Клиент сети Microsoft: использовать цифровую подпись (всегда)	Не опр
у во политики провенасности на служ Колтики провенасности на служ	📓 Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Не опр
Конфигурация расширенной полит	III Клиент сети Microsoft: отправлять незашифрованный пароль сторонним SMB-серверам	Не опр
> III QOS На ОСНОВЕ ПОЛИТИКИ	Консоль восстановления: разрешить автоматический вход администратора	Не опр
> Датинистративные шаблоны, получены о Настройка.	Консоль восстановления: разрешить копирование лискет и доступ ко всем лискам и папкам	Неопр
	Контродлер домена: запретить изменение парода учетных записей компьютера	Неопр
 Конфинурация пользователя Политики 	Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию	Не опр
Настройка	Партоналер домена: требование инфровой подписи для I DAD-сервера	Не опр
	Парторы улатына просовлике цифровон подписи для сорегорода	He onn Y
< >	с составлять составлять в призализация составлятися в файл или рестр на основании расположении	> >

11. Установите флажок Определить следующий параметр политики.

12. Установите переключатель в положении Включен.

13. Нажмите **ОК**.

Свойства: Интерактивный вход в о	систему: треб	бовать с	?	×
Параметр политики безопасности	Объяснение			
Интерактивный вход в сис	тему: требова	пъ смарт-карт	у	
Определить следующий парам	етр политики:			
• Включен				
Отключен				
	ОК	Отмена	Примен	нить

14. В окне Редактор управления групповыми политиками нажмите на пункт Конфигурации Windows.

- 15. Нажмите на подпункт Параметры безопасности.
- 16. Нажмите на пункт Локальные политики.

17. Щелкните по подпункту Параметры безопасности.

 Щелкните правой кнопкой мыши по политике Интерактивный вход в систему: поведение при извлечении смарт-карты и выберите пункт С войства.



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.
- 24. Перезагрузите компьютер.

Настройка клиентской операционной системы

Компьютеры с установленными клиентскими операционными системами Windows 11/10/8.1/8/7/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 11/10/8.1/8/7/Vista для блокировки рабочего стола при отключении устройства Рутокен необходимо установить автоматический запуск службы Политика удаления смарт-карт/Smart Card Removal Policy).