

ESMART Token – Citrix XenDesktop



Содержание

1.	Общая информация
1.1	Тестовая среда
2.	Подготовка инфраструктуры РКІ
2.1	Подготовка контроллера домена и центра выдачи сертфиикатов
2.2	Необходимые компоненты
3.	Настройка ХМL-запросов
4.	Настройка защищенного соединения 4
4.1	Настройка IIS для серверов StoreFront 4
4.2	Получение сертификата web-сервера4
4.3	Привязка сертификата к IIS5
5.	Настройка методов авторизации6
5.1	Предварительные этапы
5.2	Создание объекта Citrix Store
5-3	Настройка StoreFront
5.4	Проверка аутентификации по сертификатам
6.	Групповые политики
7.	Подготовка клиентских машин 10
7.1	Проверка авторизации через Web-интерфейс10
7.2	Получение профиля для Citrix Receiver и авторизация 10



1. Общая информация

В руководстве кратко описана настройка Citrix XenDesktop для двухфакторной аутентификации при помощи смарт-карт и USB-ключей ESMART Token и ESMART Token ГОСТ. Процедура аналогична для всех поддерживаемых гипервизоров: VMWare ESX, Hyper-V, XenServer.

Необходимо разрешить передачу данных на портах TCP 80 и 443, а также на портах, которые используют компонент Citrix Licensing Service.

1.1 Тестовая среда

В руководстве описана тестовая среда со следующим программным обеспечением:

Windows Server 2012 – Инфраструктурный сервер Citrix

citrix.esmart.local

- Director
- Delivery Controller
- Studio
- StoreFront
- Licensing Service
- SQL Server

Windows 7 x64 – Эталонная машина template.esmart.local

- Virtual Delivery Agent
- Citrix Receiver
- ESMART PKI Client

Windows server 2012 – Cepbep Active Directory

Также должна быть установлена служба сертификации (Microsoft рекомендует

Windows 7 – Клиент

dc.esmart.local

устанавливать)

client.esmart.local

- Citrix Receiver
- ESMART PKI Client

Установка ESMART PKI Client описана в руководствах на сайте www.esmart.ru.

Установка ПО Citrix Desktop не описана в данном руководстве. Для установки системы следуйте руководствам и рекомендациям с сайта производителя <u>http://docs.citrix.com</u>, в том числе документации на русском языке к версии 7,5: <u>https://docs.citrix.com/ru-ru/xenapp-and-xendesktop/7-</u> <u>5.html</u> Если на серверах установлена операционная система Windows Server 2008 рекомендуется применить патч https://support.microsoft.com/en-us/kb/949538

2. Подготовка инфраструктуры РКІ

2.1 Подготовка контроллера домена и центра выдачи сертфиикатов

Инфраструктура для авторизации по смарт-картам в Microsoft Windows предполагает наличие в организации минимум одного контроллера домена и минимум одного центра выдачи сертфикатов. Для авторизации в Windows по смарт-картам на доменных устройствах и для авторизации на виртуальных или физических ПК в инфраструктуре Citrix может использоваться одна и та же смарткарта.

Развертывание домена и установка центра выдачи сертификатов в данном руководстве не описана. Используйте руководства по развертыванию центра сертификации с сайта <u>www.esmart.ru/downloads</u> или руководства от Microsoft.

2.2 Необходимые компоненты

Для авторизации по смарт-картам в инфраструктуре Citrix должны быть выполнены следующие условия:



- Наличие одного или нескольких контроллеров домена;
- Наличие одного или нескольких центров сертификации;
- Настроенный шаблон SmartCard User (Пользователь со смарт-картой) или SmartCard Logon (Вход со смарт-картой);
- Смарт-карта или USB-ключ ESMART Token с записанным сертификатом доменного пользователя.

Записать сертификат пользователя на смарт-карту можно как с помощью оснастки certmgr.msc, так и с помощью приложения ESMART PKI Client (см. **ESMART PKI Client — Руководство** администратора).

3. Настройка XML-запросов

На серверах, на которых установлены компоненты ПО Citrix XenDesktop (кроме эталонных серверных OC) необходимо разрешить выполнение XML-запросов. Для этого в консоль Windows Powershell нужно ввести следующие команды:

Set -BrokerSite -TrustRequestsSentToTheXmlServicePort \$true

Для проверки вводится команда:

Get -BrokerSite

Ожидаемый вывод:

TrustRequestsSentToTheXmlServicePort : true

4. Настройка защищенного соединения

4.1 Настройка IIS для серверов StoreFront

Для серверов, на который установлен компонент Citrix StoreFront необходимо настроить защищенное соединение по протоколу HTTPS. Для защищенного соединения используется серверная роль Internet Information Services (Microsoft IIS).

4.2 Получение сертификата web-сервера

Сертификат веб-сервера можно получить методом, описанным ниже, или с помощью раздела панели управления IIS – Управление сертификатами.

Чтобы получить сертификат сервера, откройте консоль ММСи добавьте оснастку Сертификаты » Для учетной записи компьютера » Локальный компьютер или Другой компьютер.

В оснастке Сертификаты перейдите в раздел: Личное > Сертификаты. В верхнем меню выберите Действие > Все задачи > Запросить новый сертификат.

Следуя подсказкам мастера выдачи сертификатов перейдите к окну выбора шаблонов и отметьте шаблон сертификата Веб-сервер. Задайте требуемые параметры сертификата: Служба DNS: DNS-имя сервера StoreFront (в примере citrix.esmart.local).



						ienda eepimen	No To
Запрос сертификатов			🛆 Субъект	Общие	Расширения	Закрытый ключ	Центр сертификации
Зы можете запросить следую апросить, и нажмите кнопку	цие типы сертификатов. Выберите сертификат "Заявка".	ы, которые хотите	Субъект серт сертификат. І которые могу	ификата Можно с ут испол	 пользовате описать типы назоваться в с 	ель или компьют 1 имен субъектов сертификате.	ер, для которого выпущен и указать альтернативные
Политика регистрации Ас	tive Directory		Субъект серт	ификата Били ко	MOLHOTED DO	лучающий септи	фикат
🗹 Веб-сервер	 Остояние: Доступно 	Подробности	Имя субъекта	8	interest interest inte	ng taroagan cepin	4 mail
Требуется больше	данных для подачи заявки на этот сертификат.	Щелкните здесь для	Тип:				
- настроики параме	rpos.		Полное имя	DN	~	Добавить >	
Компьютер	(j) Состояние: Доступно	Подробности	Значение:			< Удалить	
			Дополнитель	ное имя	е]		C
			Тип:				citrix esmartilocal
Показать все шаблоны			Служба DNS	5			
			Значение:			Добавить >	
	[Заявка Отм				< Удалить	I.

Дождитесь сообщения об успешной выдаче сертификата. Полученный сертификат сервера появится в оснастке Сертификаты консоли ММС.

4.3 Привязка сертификата к IIS

Откройте Диспетчер серверов и выберите роль IIS. В настройках Default Web Site выберите Привязки...

	Andreidep chysions	
	сайты\Default Web Site	- 🛱 🗟 🖗 🛛
Файл Режим С	правка	
Подключения	📕 🚳 Начальная страница Default Web Site	Действия
В.• Начальная сто.	3844	Проводник Редактировать
CITRIX (ESM	Привязки сайта ? 🗴	разрешения
- 🔝 Пулы при	Тип Иничала Полт Валоса Селения с при	Изменение веб-сайта
Defaul	http 80 *	Основные настройки
	Добавление привязки сайта ? Х	Просмотреть
	Durins -	приложения Просмотреть
	https v Bce неназначенные v 443	виртуальные каталоги
	Unit year	Управление веб-сайтом 🙆
		🖉 Перезапустить
	Требовать обозначение имени сервера	запустить Остановить
		Обзор веб-сайта
	SSL-сертификат:	O6sop *:80 (http)
	сіtrix.esmart.local ч Выбрать Вид	Дополнительные
	крыть	параметры
	ОК Отмена	Трассировка
		i processip ourse
		невыполненных
	Просмотр возможностей	невыполненных запросов Ограничения
п	Э Просмотр возможностей 🚓 Просмотр содержимого	невыполненных запросов Ограничения
ш	 Просмотр возможностей СПросмотр содержимого 	невыполненных запросое Ограничения
ш	Просмотр возможностей Просмотр содержимого Привязки сайта	еневыполненных запросое Ограничения
отоеность	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Седения о при	невыполненных запросов Ограничения
ш	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла http 80	евыполненных запросов Ограничения
ш	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	евыполненных запросов Ограничения 2 х Добавить Изменить
ш	Э Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	евыполненных запросов Ограничения 2 х Добавить Изменить Удалить
ш	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	Ревыполненных запросов Ограничения Добавить Изменить Удалить Обзор
ш	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	евыполненных запросов Ограничения 2 Х Добавить Изменить Удалить Обзор
ш	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	Ревыполненных запросов Ограничения 2 Х Добавить Изменить Удалить Обзор
отоеность	Просмотр возможностей Просмотр содержимого Привязки сайта Тип Имя узла Порт IP-адреса Сведения о при http 80 * https citrix.esmart.local 443 *	Ревыполненных запросов Ограничения 2 Х Добавить Изменить Удалить Обзор

После выполнения привязки необходимо отметить опцию Требовать SSL в разделе Параметры SSL.



5. Настройка методов авторизации

5.1 Предварительные этапы

Предварительно требуется создать и настроить в Citrix Studio:

- Machine Catalog (в примере MC1);
- Delivery Group (в примере DG1).

Для Delivery Group должен быть назначен по крайней мере один StoreFront сервер и создан тип Store.

5.2 Создание объекта Citrix Store

В оснастке Citrix StoreFront перейдите на вкладку Stores. Начните создание нового объекта Store. Задайте его имя и перейдите к добавлению Delivery Controller. В типе транспорта укажите HTTPS и номер порта 443. Добавьте в список серверы, на которые установлен компонент Delivery Controller.

Display name:	Controller
Type:	• XenApp 7.5 (or later), or XenDesktop
	XenApp 6.5 (or earlier)
	AppController
	○ VDI-in-a-Box
Convers	citeix compet local
(load balanced):	citrixesmartilocal
	Add Edit Remove
Transport type:	HTTPS 👻
Port:	443



При необходимости добавьте шлюз NetScaler Gateway для удаленного доступа (с использованием VPNсоединения или без). В настройках NetScaler Gateway можно указать первичную авторизацию по смарт-картам и вторичную авторизацию, например, по логину и паролю (как показано на рисунке).

	-			
StoreFront	Remote Access			
	Add NetScaler Gateway a	ppliances to provide user access f	rom external ne	tworks.
✔ Store Name	Remote access:	None		
Delivery Controllers		🔘 No VPN tunnel 🚺		
Remote Access		Full VPN tunnel 1		
	NetScaler Gateway applia	inces: 🗹 ra		A
	Add NetScal	ler Gateway Appliance		
StoreFront	Add NetScal General Settings	ler Gateway Appliance		
StoreFront	Add NetScal General Settings The display name is visibl	ler Gateway Appliance	ences.	
StoreFront General Settings	Add NetScal General Settings The display name is visibl Display name:	ler Gateway Appliance le to users in Citrix Receiver prefer RemoteAccessTest	ences.	
StoreFront General Settings Secure Ticket Authority	Add NetScal General Settings The display name is visibl Display name: NetScaler Gateway URL:	ler Gateway Appliance le to users in Citrix Receiver prefer RemoteAccessTest https://citrix.esmart.local	ences.	
StoreFront General Settings Secure Ticket Authority	Add NetScal General Settings The display name is visibl Display name: NetScaler Gateway URL: Version:	ler Gateway Appliance le to users in Citrix Receiver prefer RemoteAccessTest https://citrix.esmart.local 10.0 (Build 69.4) or later	ences.	
StoreFront General Settings Secure Ticket Authority	Add NetScal General Settings The display name is visibl Display name: NetScaler Gateway URL: Version: Subnet IP address: (optional)	ler Gateway Appliance le to users in Citrix Receiver prefer RemoteAccessTest https://citrix.esmart.local 10.0 (Build 69.4) or later SNIP or MIP	ences.	
StoreFront General Settings Secure Ticket Authority	Add NetScal General Settings The display name is visibl Display name: NetScaler Gateway URL: Version: Subnet IP address: (optional) Logon type:	ler Gateway Appliance le to users in Citrix Receiver prefer RemoteAccessTest https://citrix.esmart.local 10.0 (Build 69.4) or later SNIP or MIP Smart card	ences.	

5.3 Настройка StoreFront

Для аутентификации по смарт-картам необходимо включить данный метод в оснастке управления компонентом StoreFront. Отметьте опцию Smart Card и Domain pass-through. Остальные настройки устанавливаются в соответствии с корпоративными требованиями.





При настройке инфраструктуры, содержащей несколько серверных групп StoreFront, необходимо следовать рекомендациям Citrix (http://support.citrix.com/proddocs/topic/dws-storefront-21/dws-configure-server-group.html)

5.4 Проверка аутентификации по сертификатам

Подключите к клиентскому компьютеру считыватель со смарт-картой или USB-токен ESMART Token, на который записан доменный сертификат пользователя для авторизации в Windows. Для проверки настройки безопасного соединения по смарт-картам, перейдите в браузере Internet Explorer на следующий адрес:

https://**storefront-name**/Citrix/Authentication/Certificate/test.aspx, например: https://citrix.esmart.local/Citrix/Authentication/Certificate/test.aspx

При переходе по данной ссылке будет запрошен сертификат пользователя. Выберите сертификат, записанный на смарт-карту и введите ПИН-смарт-карты. Если авторизация прошла успешно, на странице будут показаны параметры сертификата пользователя на смарт-карте.





6. Групповые политики

На клиентские машины требуется распространить групповые политики Citrix. Файл шаблона находится в директории

C:\Program Files(x86)\Citrix\ICA Client\Configuration\icaclient.adm

Рекомендуется распространение через доменные групповые политики, но допускается и изменение локальных групповых политик.





7. Подготовка клиентских машин

7.1 Проверка авторизации через Web-интерфейс

Проверьте возможность авторизации по картам через Web-интерфейс (в браузере должно быть разрешено выполнение JavaScript):

https:// StoreFrontServer/Citrix/StorenameWeb

в примере

https://citrix.esmart.local/Citrix /ESMARTauthStoreWeb

Добавьте серверы StoreFront в настройках браузера Internet Explorer в категорию Local Zone или Trusted Zone.

7.2 Получение профиля для Citrix Receiver и авторизация

Установите Citrix Receiver на клиентский ПК. Рекомендуется установка с опцией /includeSSON AM_SMARTCARDPINENTRY=CSP

D:\Installers\CitrixReceiver.exe /includeSSON AM_SMARTCARDPINENTRY=CSP

Профиль для настройки Citrix Receiver можно получить через web-интерфейс, описанный выше. В правом верхнем углу web-страницы нажмите на имя пользователя и выберите опцию Активировать. Полученный файл будет автоматически ассоциирован с приложением Citrix Receiver. При открытии Citrix Receiver проверьте и подтвердите доверие к серверу Citrix. Запустите или перезапустите приложение Citrix Receiver. Авторизуйтесь с помощью смарт-карты на доступном рабочем столе.

