

Установка корневого сертификата SkyDNS

Корневой сертификат или сертификат SSL - одна из частей системы безопасности сайтов. Сертификат SSL необходим для корректной работы сайтов с безопасным соединением (https). Если у Вас возникают проблемы с отображением страницы блокировки SkyDNS (браузер выдает сообщение "Не удается получить доступ к сайту"), то Вам необходимо скачать сертификат SkyDNS и настроить его использование в Вашем браузере.

Скачать корневой сертификат SkyDNS

(если при переходе по ссылке браузер открывает окно установки сертификата, отмените установку, кликните по кнопке правой клавишей мыши и выберите пункт **Сохранить объект как...**)

Содержание:

 Установка сертификата SkyDNS для Windows (браузеры Internet Explorer, Edge, Opera, Google Chrome)
 Установка сертификата SkyDNS в браузере Mozilla Firefox для всех платформ
 Установка сертификата SkyDNS в Mac OSX

Чтобы проверить работу страницы блокировки в https воспользуйтесь следующей инструкцией:

4. Проверка корректности работы страницы блокировки после установки сертификата



1. Установка сертификата SkyDNS для Windows (браузеры Internet Explorer, Edge, Opera, Google Chrome)

Установка сертификата для браузеров **Internet Explorer, Edge, Opera, Google Chrome** производится через системные настройки.

Внимание! Сертификат не поддерживается в Yandex браузере.

Внимание! Браузер Mozilla Firefox не использует системные настройки, для установки сертификата воспользуйтесь <u>этой инструкцией</u>.

Шаг 1. Нажмите кнопку Пуск и начните вводить словосочетание Панель управления



Когда появится иконка Панели Управления нажмите на нее.



Шаг 2. В поиске панели управления введите Свойства браузера и нажмите появившуюся иконку.

🖭 свойства браузера - Панель управления			-	×
← → ▼ ↑ 🛃 > Панель управления >	~ Ō	свойства брау	зера	×
🐑 Свойства браузера				
Оскать "свойства браузера" в центре справки и поддержки Windows				

Шаг З. В Свойствах браузера перейдите на вкладку Содержание и нажмите кнопку Сертификаты.

🚷 Свойства: Ин	тернет			?	×		
Общие Содержание	Общие Безопасность Конс Содержание Подключения Программы				ь 16Н0		
Сертификаты Серти подкл Очистит	ификаты использук лючений и удостови ъ SSL Серти	отся для шиф ерения подли 1фикаты	рованных інности. Изда	тели	_		
Автозаполнение Вводі подхі	аполнение запомин ившиеся данные и г одящие строки.	ает ранее юдставляет	Парам	етры			
одходящие строки. Веб-каналы и веб-фрагменты предоставляюто бновляемое содержимое веб-сайтов, которое можно прочитать с помощью Internet Explorer и других программ.							
	0	к	Отмена	Приме	енить		



Шаг 4. В окне Сертификаты перейдите на вкладку Доверенные корневые центры сертификации и нажмите кнопку Импорт.

👫 Сертификаты							×
Назначение:	<bce></bce>						~
Доверенные корневы	ые центр	оы сертификации	Дов	еренные изда	атели	Издатели, не	• •
Кому выдан	к	(ем выдан		Срок де	Поня	тное имя	^
AddTrust Extern	al A	AddTrust External C	Α	30.05.2020	The l	JSERTrust	
Baltimore Cyber	Tru B	altimore CyberTrus	t	13.05.2025	DigiC	ert Baltimor	
Certum CA	C	Certum CA		11.06.2027	Cert	um	
Certum Trusted	Ne C	Certum Trusted Netv	v	31.12.2029	Certum Trusted		
Class 3 Public Pri	ima C	Class 3 Public Primary		02.08.2028	VeriSign Class 3		
Copyright (c) 19	97 C	Copyright (c) 1997 Mi		31, 12, 1999	Microsoft Timest		
🔄 DigiCert Global R	D	DigiCert Global Root CA		10.11.2031	DigiC	lert	
DigiCert High As	sur D	DigiCert High Assuran		10.11.2031	DigiC	ert	
DST Root CA X3	D	OST Root CA X3		30.09.2021	DST	Root CA X3	¥
Импорт Эксг	юрт	Удалить			[Дополнител	ьно
Назначения сертифи	ката						
						Просмот	.b
						Закрыть	

Шаг 5. В окне мастера импорта сертификатов на первом шаге нажмите кнопку Далее.

🗧 🍃 Мастер импорта сертификатов	×
Мастер импорта сертификатов	
Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.	
Для продолжения нажмите кнопку "Далее".	
Далее Отме	на



Шаг 6. На втором шаге нажмите кнопку Обзор и выберите заранее загруженный файл сертификата SkyDNS.

 Мастер импорта сертификатов Импортируемый файл Укажите файл, который вы хотите импортировать.
Импортируемый файл Укажите файл, который вы хотите импортировать.
Импортируемый файл Укажите файл, который вы хотите импортировать.
Укажите файл, который вы хотите импортировать.
имя фаила:
C:\Users\user\Downloads\skydns.cer O63op
Замечание: следующие форматы файлов могут содержать более одного сертификата в одном файле:
Файл обмена личной информацией - PKCS #12 (.PFX,.P12)
Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
Хранилище сериализованных сертификатов (.SST)
Далее Отмена



Шаг 7. На третьем шаге убедитесь, что сертификат помещается в хранилище **Доверенных корневых центров сертификации.**

	×
🗧 😺 Мастер импорта сертификатов	
Yosuu nuus contucturaton	
Хранилища сертификатов - это системные области, в которых	
хранятся сертификаты.	
Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.	
О Автоматически выбрать хранилище на основе типа сертификата	
• Поместить все сертификаты в следующее хранилище	
Хранилище сертификатов:	
Доверенные корневые центры сертификации Обзор	
Далее Отмен	на



Шаг 8. Подтвердите ранее проделанные действия, нажав на кнопку Готово.

÷	Ş	Мастер импорта сертификатов		Х
		Завершение мастера импорта серти	фикатов	
		Сертификат будет импортирован после нажатия кнопк	1 "Готово".	
		Были указаны следующие параметры:		
		Хранилище сертификатов, выбранное пользователем Содержимое	Доверенные корневые цент Сертификат	
		Файл	C: \Users\user\Downloads\sk\	
		<	>	
			Готово Отмен	ia

Шаг 9. На вопрос системы нужно ответить Да.

🍖 Пред	упреждение системы безопасности	×
	Будет установлен сертификат от центра сертификации (ЦС), представляющий:	
	SkyDNS Root CA	
	Windows не удается проверить, что сертификат действительно получен от "SkyDNS Root CA". Обратитесь к "SkyDNS Root CA" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:	
	Отпечаток (sha1) : 4EFBA278 A55E213E 06FD4199 5285F0F2 3CA36293	
	Предупреждение: Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.	
	Вы хотите установить этот сертификат?	
	Да Нет	



Шаг 10. Закрыть мастер импорта сертификатов, нажав Ок.





2. Установка сертификата SkyDNS в браузере Mozilla Firefox для всех платформ

Браузер Mozilla Firefox не использует системные настройки, поэтому установка сертификата в нем отличается от других браузеров.

Шаг 1. Щелкните по иконке настроек в правом верхнем углу браузера и выберите пункт меню Настройки.

		1	•	
C	Войти в Синхронизацию			
Ģ	Новое окно		C	trl+N
8	Новое приватное окно	С	trl+Sh	ift+P
Ģ	Восстановить предыдущу	юс	ессию	0
	Масштаб — 100%		+	ĸ۵
	Правка 🐰		ዔ	Ê
lii\	Библиотека			>
ġ.	Дополнения	C	trl+Sh	ift+A
₽	Настройки			
	Изменить			
	Открыть файл		C	trl+0
	Сохранить как		C	trl+S
=	Печать			
۹	Найти на этой странице		C	trl+F
	Больше			>
	Веб-разработка			>
?	Справка			>
Ф	Выход	C	trl+Sh	ift+Q



Шаг 2. В левом меню выберите **Приватность и защита** затем прокрутите в самый низ страницы и нажмите кнопку **Просмотр сертификатов**.

🗱 Настройки	× +
← → ♂ ଢ	Sirefox about:preferences#privacy
	Р Найти в настройках
🔅 Основные	Подробнее
Q Поиск	Разрещить Firefox отправлять сообщения о падениях в Mozilla Подробнее
Приватность и Защита	Защита
Аккаунт Firefo	Поддельное содержимое и защита от вредоносных программ
	 Бдокировать опасное и обманывающее содержимое Подробнее
	 Блокировать опасные загрузки
	Предупреждать о нежелательных и нетипичных программах
	Сертификаты
	Когда сервер запрашивает личный сертификат
	Отпр <u>а</u> влять автоматически
	Спращивать каждый раз
	За <u>п</u> рашивать у OCSP-серверов подтверждение текущего Просмотр сертификатов
Поддержка Firefox	статуса сертификатов Устройства защиты

Шаг З. В окне Сертификатов выберите вкладку Центры сертификации и нажмите кнопку Импортировать.

			Управление сертификатами		
Ваши сертифик	аты Люди	Серверы	Центры сертификации	Другие	
/ вас хранятся сер	тификаты, служаг	цие для иденти	ификации следующих центров	з сертификации	
Имя сертификата			Устройство за	щиты	Ę
AC Camerfirma S.A.					
Chambers of Comm	erce Root - 2008		Builtin Object Token		
Global Chambersign	Root - 2008		Builtin Object Token		
AC Camerfirma SA CIF	A82743287				
Camerfirma Chamb	ers of Commerce Root		Builtin Object Token		
Camerfirma Global (Chambersign Root		Builtin Object Token		
ACCV					
ACCVRAIZ1			Builtin Object Token		
Actalis S.p.A./03358520	967				
Actalis Authenticatio	n Root CA		Builtin Object Token		
AddTrust AB					
Пр <u>о</u> смотреть	Изм <u>е</u> нить дове	рие И <u>м</u> п	ортировать Экс <u>п</u> ортиро	вать Уда <u>л</u> ить или не доверять	
					OK
					OK



Шаг 4. Выберите заранее загруженный сертификат SkyDNS. В окне загрузки сертификата установите галочку Доверять при идентификации веб-сайтов и нажмите кнопку ОК.

Загрузка сертификата	\times
Вам предлагают доверять новому центру сертификации (СА).	
Вы хотите доверять «SkyDNS Root CA» для следующих назначений?	
🗹 Доверять при идентификации веб-сайтов.	
🗌 Доверять при идентификации пользователей электронной почты.	
🗌 Доверять при идентификации производителей программного обеспечения.	
Перед тем, как определиться с доверием к этому центру, рекомендуется проверить его сертификат, политику и процедуры (если возможно).	
Просмотреть Проверить сертификат центра	
ОК Отмена	



3. Установка сертификата SkyDNS в Mac OSX

Шаг 1. Нажмите сочетание клавиш CTRL+SPACE и в поиске Spotlight введите "Связка ключей". Откройте приложение Связка ключей.

ТОП-РЕЗУЛЬТАТЫ	
🔏 - Сеязка ключей	
О Ассистент обратной связи	
О Сеть	
СИСТЕМНЫЕ НАСТРОЙКИ	
i iCloud	178
	a (; v
	Bencker 10.0
	bepont. Toto
	Тип Поограмма
	Создано 03.10.2017
	Изменено 15.01.2018
	Последнее открытие 17.01.2018

Шаг 2. В приложении Связка ключей выберите параметр **Вход** и категорию **Сертификаты**.

		Связка ключей			
Нажмите, чтобы з	акрыть доступ к связке ключей «Вход	»,		Q Поис	ĸ
Связки ключей					
🧉 Вход					
C iCloud					
🔒 Система					
[] Центрификации					
	Имя	^	Тип	Срок действия	Связка клю
			Сертификат	21 окт. 2026 г., 5:00:00	Вход
			Сертификат	8 февр. 2023 г., 2:48:47	Вход
	▶ 🔛		Сертификат	29 нояб. 2019 г., 18:50:42	Вход
			Сертификат	2 февр. 2027 г., 3:12:15	Вход
	► 🔄	and the second second	Сертификат	28 нояб. 2018 г., 11:06:29	Вход
	► 📴		Сертификат	20 дек. 2018 г., 11:36:01	Вход
	► 🖼		Сертификат	28 дек. 2018 г., 11:52:02	Вход
Категория					
\Lambda Все объекты					
🦾 Пароли					
Секретные заме					
🔄 Мои сертификаты					
Ключи					
Сертификаты					
	(+) Скопировать		Объектов: 7		



Шаг 3. Перетащите заранее загруженный сертификат SkyDNS в правую часть окна приложения Связка ключей, где хранятся остальные сертификаты.

• • •		Связка ключей			
Нажмите, чтобы з	акрыть доступ к связке ключей	і́ «Вход».		Q. Поис	к
Связки ключей Вход Cloud Cистема Система Система	Сентрале Корневое бюр Истекает: пон © Данный кор	ot CA ю сертификации едельник, 10 января 2028 г., 14:57:2/ невой сертификат ненадежен	0 Екатеринбург, ст	гандартное время	
	Имя	^	Тип	Срок действия	Связка клю
			Сертификат	21 окт. 2026 г., 5:00:00	Вход
			Сертификат	8 февр. 2023 г., 2:48:47	Вход
			Сертификат	29 нояб. 2019 г., 18:50:42	Вход
			Сертификат	2 февр. 2027 г., 3:12:15	Вход
	► 5		Сертификат	28 нояб. 2018 г., 11:06:29	Вход
			Сертификат	20 дек. 2018 г., 11:36:01	Вход
	▶ 🔤		Сертификат	28 дек. 2018 г., 11:52:02	Вход
Категория	SkyDNS Root CA		Сертификат	10 янв. 2028 г., 14:57:20	Вход
 Все объекты Пароли Секретные заме Мои сертификаты Ключи 					
📴 Сертификаты					
	+ і Скопировать		Объектов: 8		

Шаг 4. Щелкните правой кнопкой мыши по сертификату SkyDNS и выберите пункт меню Свойства сертификата. В открывшемся окне разверните пункт Доверие и в Параметрах использования сертификата выберите "Всегда доверять". Закройте окно сертификата.

	SkyDNS F	SkyDNS Root CA			
SkyDNS Root CA Корневое бюро сертификации Истекает: понедельник, 10 января 2028 г., 14:57:20 Екатеринбург, стандартное время Данный корневой сертификат ненадежен					
▼ Доверие					
Парамет	ры использования сертификата:	Всегда доверять ᅌ ?			
Проток	ол защищенных сокетов (SSL)	Всегда доверять			
	Безопасная почта (S/MIME)	Всегда доверять			
Расширяемая аутентификация (ЕАР)		Всегда доверять ᅌ			
	IP-безопасность (IPsec)	Всегда доверять ᅌ			
	Подпись кода	Всегда доверять 🗘			
1	Трисвоение временных меток	Всегда доверять ᅌ			
Стандартный алгоритм Х.509		Всегда доверять ᅌ			
▼ Подробнее					
	Тема				
	Страна RU				
	Штат/территория Russia				
Населенный пункт_Yekaterinburg					



Шаг 5. В приложении Связка ключей убедитесь, что сертификат SkyDNS помечен как надежный для данной учетной записи.

•••		Связка ключей				
Нажмите, чтобы закрыть доступ к связке ключей «Вход».			Q. Поиск			
Связки ключей Вход iCloud Cистема Центрификации	Сенфект Корневое бюро серт Истекает: понедельн Оданный сертифика	ификации ик, 10 января 2028 г., 14:57:20 ат помечен как надежный для) Екатеринбург, ст этой учетной запі	андартное в иси	ремя	
	Имя	^	Тип	Срок д	ействия	Связка клю
			Сертификат	21 окт.	2026 г., 5:00:00	Вход
			Сертификат	8 февр	. 2023 г., 2:48:47	Вход
			Сертификат	29 ноя	5. 2019 r., 18:50:42	Вход
			Сертификат	2 февр.	2027 г., 3:12:15	Вход
			Сертификат	28 ноя	5. 2018 r., 11:06:29	Вход
	► 🔤		Сертификат	20 дек.	2018 r., 11:36:01	Вход
	▶ 🔤		Сертификат	28 дек.	2018 r., 11:52:02	Вход
Категория	🛐 SkyDNS Root CA		Сертификат	10 янв.	2028 г., 14:57:20	Вход
 Все объекты Пароли Секретные заме Мои сертификаты Ключи Сертификаты 						
	+ і Скопировать		Объектов: 8			



4. Проверка корректности работы страницы блокировки после установки сертификата

Теперь можно проверить блокировку сайтов по протоколу **https**. При попытке зайти на заблокированный сайт у Вас должна отобразиться страница блокировки. Если страница блокировки не отображается, либо отображается оповещение браузера о недействительном сертификате - повторите шаги по установке сертификата.

Если после повторной настройки останутся нерешенные вопросы или проблемы - обращайтесь в нашу службу технической поддержки.