

# Настройки групповых политик контроля учетных записей в Windows 7

oszone.net/11424

Существует 10 настроек групповой политики, отвечающих за настройку контроля учетных записей пользователей. Для того, чтобы изменить параметры политики, нужно открыть в оснастке «Редактор локальной групповой политики» узел **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Параметры безопасности**. В этой статье вы также найдете способ настройки каждого параметра политики средствами системного реестра. В следующей таблице приведены значения по умолчанию для каждого из параметров политики.

Настройки параметров групповых политик контроля учетных записей по умолчанию:

Параметр групповой политики	Значение по умолчанию
Контроль учетных записей: включение режима одобрения администратором	Включен
Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав	Включен
Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав	Включен
Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором	Запрос согласия для двоичных данных не из Windows
Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей	Запрос учетных данных
Контроль учетных записей: повышать права только для UIAccess-приложений, установленных в безопасном местоположении	Включен
Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в размещение пользователя	Включен
Контроль учетных записей: разрешать UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол	Отключен
Контроль учетных записей: использование режима одобрения администратором для встроенной учетной записи администратора	Отключен

Параметры групповых политик, которые имеют отношение к контролю учетных записей пользователей (UAC) подробно рассмотрены ниже:

## Все администраторы работают в режиме одобрения администратором

Этот параметр политики определяет характеристики всех политик контроля учетных записей для компьютера. От данного параметра зависит, будут ли учетные записи администраторов запускаться в «режиме одобрения администратором», то есть будут ли отображаться диалоги с запросом на повышение полномочий. Отключение этой настройки, грубо говоря, полностью отключает функционал контроля учетными записями пользователей. При изменении этого параметра политики необходимо перезагрузить компьютер. Значение по умолчанию – включено.

Возможные значения параметра:

- **Включено.** Режим одобрения администратором включен для того, чтобы разрешить встроенной учетной записи администратора и всем остальным пользователям, являющимся членами группы **«Администраторы»**, работать в режиме одобрения администратором.
- **Отключено.** Режим одобрения администратором и все соответствующие параметры политики контроля учетных записей будут отключены.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"EnableLUA"=dword:00000000
```

## Обнаружение установки приложений и запрос на повышение прав

---

Эта настройка определяет характеристики обнаружения установки приложений для компьютера, проверяя подписаны ли программы, применяемые для развертывания приложений или нет. По умолчанию, если пользователь входит в рабочую группу, она включена.

Возможные значения параметра:

- **Включено (по умолчанию для дома).** В том случае, если программа установки приложений обнаруживает необходимость повышения полномочий, пользователю предлагается ввести имя пользователя и пароль учетной записи администратора. Если пользователь вводит правильные учетные данные, операция продолжается с соответствующими правами. Вид запроса зависит от того, к какой группе принадлежит пользователь.
- **Отключено (по умолчанию для организации).** При выборе этой настройки, обнаружение программы установки приложений не выдает запрос на повышение полномочий. Обычно эта настройка применяется в организациях, компьютеры и пользователи которой входят в состав домена и для развертывания приложений используются технологии делегированной установки (Group Policy Software Install - GPSI). Соответственно, необходимость в обнаружении установщика отпадает.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"EnableInstallerDetection"=dword:00000000
```

## Переключение к безопасному рабочему столу при выполнении запроса на повышение прав

---

Данный параметр политики определяет, будут ли запросы на повышение полномочий выводиться на интерактивный рабочий стол пользователя или на безопасный рабочий стол при инициировании UAC-запроса. Значение по умолчанию – включено. При изменении этого параметра политики необходимо перезагрузить компьютер.

Возможные значения параметры:

- **Включено.** Все запросы на повышение прав выводятся на безопасный рабочий стол независимо от параметров политики поведения приглашения для администраторов и обычных пользователей.
- **Отключено.** Все запросы на повышение прав выводятся на интерактивный рабочий стол пользователя.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"PromptOnSecureDesktop"=dword:00000000
```

## Поведение запроса на повышение прав для администраторов в режиме одобрения администратором

---

Текущая настройка позволяет определить действия пользователя, который входит в группу **«Администраторы»** при выполнении операции, требующей повышения прав. Значение по умолчанию установлено **«Запрос согласия для сторонних двоичных файлов (не Windows)»**.

Возможные значения параметра:

- **Повышение без запроса.** Позволяет привилегированным учетным записям выполнить операцию, требующую повышения прав, без подтверждения согласия или ввода учетных данных. Желательно использовать данную опцию только в средах с максимальными ограничениями пользователей. При выборе этой настройки, пользовательские полномочия станут идентичными встроенной учетной записи администратора.
- **Запрос учетных данных на безопасном рабочем столе.** Для любой операции, требующей повышения прав, на безопасном рабочем столе будет выводиться предложение ввести имя и пароль привилегированного пользователя. Если вводятся правильные учетные данные, операция будет продолжена с максимальными доступными правами пользователя.
- **Запрос согласия на безопасном рабочем столе.** Для любой операции, требующей повышения прав, на безопасном рабочем столе будет выводиться

предложение выбрать: **«Разрешить»** или **«Запретить»**. При выборе опции **«Разрешить»**, операция будет продолжена с максимальными доступными правами пользователя.

- **Запрос учетных данных.** Для любой операции, которая требует повышения полномочий, будет выводиться предложение ввести имя пользователя и пароль учетной записи администратора. При вводе правильных учетных данных, операция будет продолжена с повышенными полномочиями.
- **Запрос согласия.** При выборе этой опции, для любой операции, требующей повышения прав, пользователю будет предлагаться выбрать нажать на кнопку: **«Разрешить»** или **«Запретить»**. При нажатии на кнопку **«Разрешить»**, операция будет продолжена с максимальными доступными привилегиями пользователя.
- **Запрос согласия для сторонних двоичных файлов (не Windows).** При выборе этой опции, на безопасном рабочем столе будет выводиться предложение выбора: **«Разрешить»** или **«Запретить»**, в том случае, когда операция для приложения стороннего (не Майкрософт) производителя требует повышения прав. По нажатию на кнопку **«Разрешить»**, операция будет продолжена с максимальными доступными привилегиями пользователя.

Настройки текущей политики при помощи реестра:

```
;Повышение без запроса
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"ConsentPromptBehaviorAdmin"=dword:00000000
;Запрос учетных данных на безопасном рабочем столе
;"ConsentPromptBehaviorAdmin"=dword:00000001
;Запрос согласия на безопасном рабочем столе
;"ConsentPromptBehaviorAdmin"=dword:00000002
;Запрос учетных данных
;"ConsentPromptBehaviorAdmin"=dword:00000003
;Запрос согласия
;"ConsentPromptBehaviorAdmin"=dword:00000004
;Запрос согласия для двоичных данных не из Windows
;"ConsentPromptBehaviorAdmin"=dword:00000005
```

## Поведение запроса на повышение прав для обычных пользователей

Данный параметр политики определяет выполняемые действия при взаимодействии обычного пользователя с приложениями, требующими повышения прав. Значение по умолчанию – **«Запрос учетных данных на безопасном рабочем столе»**.

Возможные значения параметра:

- **Запрос учетных данных.** Используя этот параметр, обычному пользователю предлагается выбрать учетную запись администратора и ввести пароль для выполнения последующих действий. Операция будет продолжена только в том случае, если учетные данные введены правильно.
- **Автоматически запретить запросы на повышение прав.** При выборе этого параметра, для обычного пользователя будет показано сообщение об ошибке в

связи с запретом на доступ в случае выполнения операции, требующей повышения полномочий. Организации, настольные компьютеры которых используются обычными пользователями, могут выбрать этот параметр политики для уменьшения числа обращений в службу поддержки.

- **Запрос учетных данных на безопасном рабочем столе.** Выбрав данный параметр, обычному пользователю предлагается выбрать учетную запись администратора и ввести пароль для выполнения последующих действий только на безопасном рабочем столе. Операция будет продолжена только в том случае, если учетные данные введены правильно.

Настройки текущей политики при помощи реестра:

```
;Автоматически отклонять запросы на повышение прав  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"ConsentPromptBehaviorUser"=dword:00000000  
;Запрос учетных данных на безопасном рабочем столе  
"ConsentPromptBehaviorUser"=dword:00000001  
; Запрос учетных данных  
"ConsentPromptBehaviorUser"=dword:00000003
```

## Повышать права для UIAccess-приложений только при установке в безопасных местах

---

Текущий параметр политики позволяет управлять разрешением на местонахождение приложений, которые запрашивают выполнение на уровне целостности, определяющейся атрибутом пользовательского интерфейса доступа (User Interface of Access - UIAccess) в безопасном месте файловой системы. По умолчанию, эта настройка включена и у приложений со специальными возможностями, для атрибута UIAccess в манифесте устанавливается значение True для управления окна запроса повышения привилегий. Если у приложений значение false, то есть если атрибут опущен или отсутствует манифест для сборки, приложение не сможет получить доступ к защищенному пользовательскому интерфейсу. Безопасными считаются только следующие папки:

...\Program Files\, включая вложенные папки

...\Windows\system32\

...\Program Files (x86)\, включая вложенные папки для 64-разрядных версий Windows

Возможные значения параметра:

- **Включено.** Приложение будет запускаться с уровнем целостности UIAccess только в том случае, если оно находится в безопасной папке файловой системы.
- **Отключено.** Приложение будет запускаться с уровнем целостности UIAccess, даже если оно не находится в безопасной папке файловой системы.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"EnableSecureUIAPaths"=dword:00000000
```

## Повышение прав только для подписанных и проверенных исполняемых файлов

---

Данная настройка групповой политики контроля учетных записей позволяет определять, нужно ли выполнять проверку подлинности подписей интерактивных приложений с инфраструктурой открытого ключа (Public key infrastructure PKI), которые требуют повышения полномочий. Задачей PKI является определение политики выпуска цифровых сертификатов, выдача их и аннулирование, хранение информации, необходимой для последующей проверки правильности сертификатов. В число приложений, поддерживающих PKI, входят: защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной цифровой подписью. Если включена эта проверка, то программы инициируют проверку пути сертификата. Значение этой настройки по умолчанию – Отключено.

Возможные значения параметра:

- **Включено.** Принудительно инициируется проверка пути PKI-сертификатов, прежде чем запускается на исполнение данный файл. В основном данная настройка используется в организациях с доменом, в том случае если администратор поместил PKI-сертификаты в хранилище надежных издателей.
- **Отключено.** При установке этого параметра, контроль учетных записей не инициирует проверку цепочки верификации PKI-сертификатов, прежде чем разрешить выполнение данного исполняемого файла.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"ValidateAdminCodeSignatures"=dword:00000000
```

## При сбоях записи в файл или реестр виртуализация в место размещения пользователя

---

Этот параметр управляет перенаправлением сбоев записи приложений в определенные расположения в реестре и файловой системе. В случае, если эта настройка включена, для устаревших приложений, которые пытаются считывать или записывать информацию, используя защищенные области системы, контроль учетных записей виртуализирует реестр и файловую систему. Благодаря этой настройке, UAC позволяет уменьшить опасность устаревших приложений, которые выполняются от имени администратора и во время выполнения записывают данные в папку %ProgramFiles%, %Windir%; %Windir%\system32 или в раздел системного реестра HKLM\Software\. Значение по умолчанию – включено.

Возможные значения параметра:

- **Включено.** Сбои записи приложений перенаправляются во время выполнения в определенные пользователем расположения в файловой системе и реестре.
- **Отключено.** Выполнение приложений, записывающих данные в безопасные расположения, заканчивается ошибкой, и не будет исполняться.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"EnableVirtualization"=dword:00000000
```

## Разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол

Этот новый параметр политики, появившийся в операционных системах Windows 7 и Windows Server 2008 R2, определяет, могут ли UIAccess-приложения автоматически отключать безопасный рабочий стол для запросов на повышение полномочий, используемых обычным пользователем. Значение по умолчанию – отключено.

Возможные значения параметра:

- **Включено.** При выборе этой настройки, UIAccess-программы, в том числе удаленный помощник Windows, автоматически отключают безопасный рабочий стол для запросов на повышение полномочий. Если параметр политики **«Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав»** включен, то предложение появится на интерактивном рабочем столе пользователя, а не на безопасном рабочем столе.
- **Отключено.** При выборе этого параметра, безопасный рабочий стол может быть отключен только пользователем интерактивного рабочего стола или путем отключения параметра политики **«Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав»**.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"EnableUIADesktopToggle"=dword:00000000
```

## Режим одобрения администратором для встроенной учетной записи администратора

Данная настройка определяет, применяется ли в контроле учетных записей пользователей режим одобрения администратором к встроенной учетной записи **«Администратор»**. Эта встроенная учетная запись по умолчанию позволяет пользователю входить в систему в режиме совместимости с Windows XP, что разрешает запускать любые приложения с полными правами администратора. По умолчанию этот параметр политики отключен.

Возможные значения параметра:

- **Включено.** При выборе этого значения параметра, для встроенной учетной записи администратора будет использоваться режим одобрения администратором. При этом любая операция, требующая повышения прав, будет сопровождаться запросом на подтверждение операции.
- **Отключено.** Встроенная учетная запись администратора выполняет все приложения с полными правами администратора.

Настройки текущей политики при помощи реестра:

```
;Отключить  
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]  
"FilterAdministratorToken"=dword:00000000
```

## Заключение

---

В этой статье рассказывается обо всех возможных настройках контроля учетных записей пользователей. Рассмотрены все десять параметров политики безопасности, которые отвечают за все возможные действия, связанные с UAC. Кроме настройки контроля учетных записей при помощи групповой политики, также рассмотрены эквивалентные им твики реестра.

**Автор:** [Dmitry\\_Bulanov](#) • **Источник:** [dimanb.spaces.live.com](#) • **Опубликована:** 16.02.2010