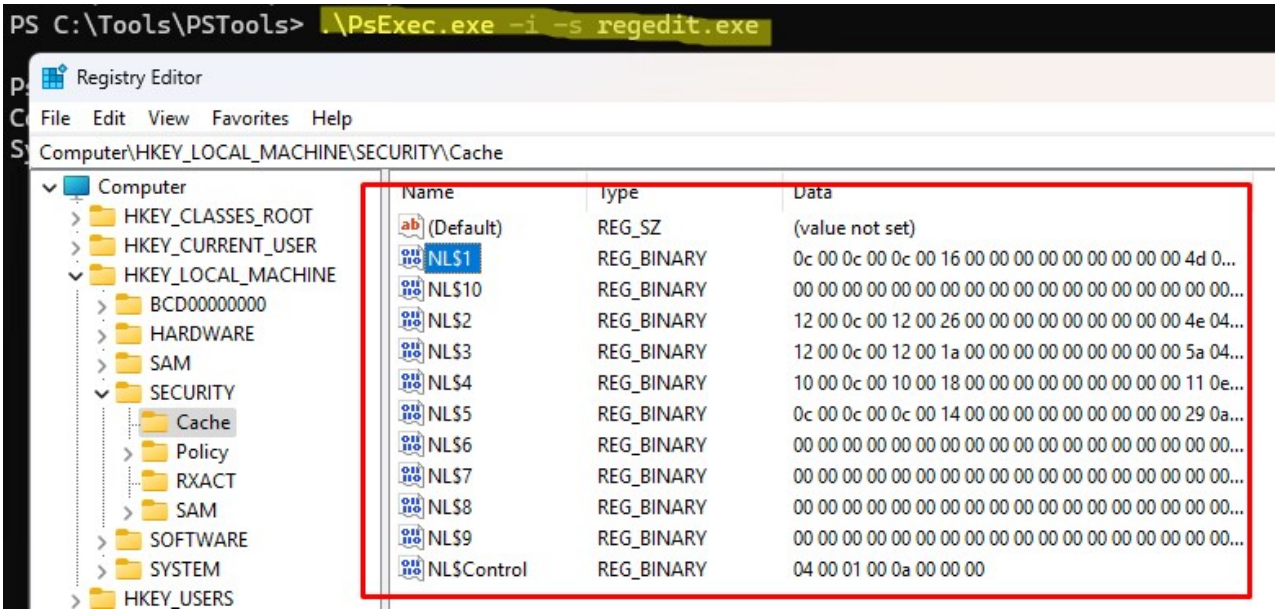
Cached Credentials: вход в Windows под сохраненными учетными данными при недоступности домена

winitpro.ru/index.php/2020/11/16/cached-credentials-windows-cashedlogonscount

itpro



Windows по умолчанию сохраняет (кэширует) учетные данные доменных пользователей при успешном входе на компьютер. Благодаря этому пользователь сможет войти на свой компьютер под своим доменным аккаунтом, даже если контроллеры домена Active Directory недоступны или компьютер не подключен к сети (офлайн). В этой статье мы рассмотрим особенности использования кешированных учетных данных (Cached Credentials) пользователей в Windows

Кэширование учетных данных пользователя для входа в Windows

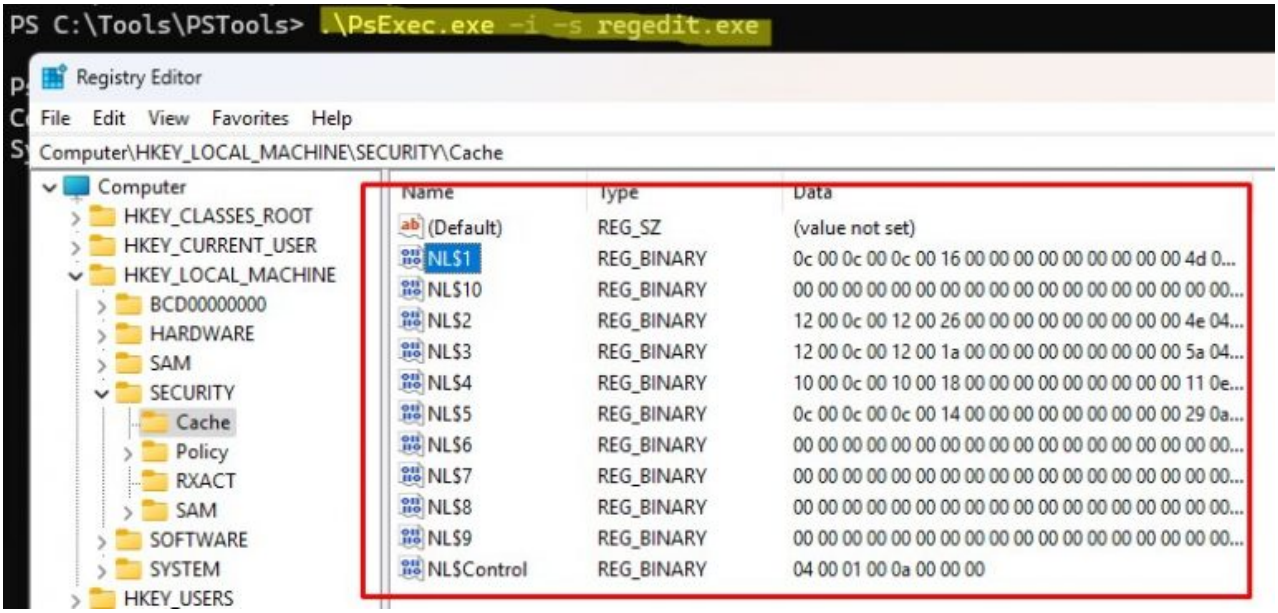
Пользователь сможет войти на оффлайн компьютер под своей доменной учетной записью, если он ранее хотя бы один раз успешно аутентифицировался на этом устройстве. При входе на доменный компьютер, хеш доменного имени пользователя и пароля сохраняются в реестре. Если домен Active Directory не доступен, Windows рассчитывает хэш введенного имени и пароля пользователя, и проверяет есть ли такой хэш в реестре. Если хеш найден, пользователю разрешается локальный вход на компьютер даже при отсутствии связи с контроллером домена.

Использование cashed credentials для входа удобно для пользователей мобильных устройств, которое могут получать доступ к своим данным на ноутбуках, даже когда отсутствует подключение к корпоративной сети.

Сохраненные пароли хранятся в ветке реестра **HKEY_LOCAL_MACHINE\Security\Cache** (файл `%systemroot%\System32\config\SECURITY`). Каждый сохранённый хэш содержится в Reg_Binary параметре **NL$x** (где x – индекс кэшированных данных).

Содержимое этой ветки реестра можно посмотреть с помощью regedit.exe, если запустить его от имени SYSTEM с помощью утилиты psexec (у администратора нет доступа к этому разделу реестра).

```
PsExec.exe -i -s regedit.exe
```



В хеше не хранятся имя и пароль доменного пользователя в открытом виде. Вместо это, на основе имени пользователя генерируется некая соль (salt), с помощью которого обрабатывается хэш пароля (используется формат **MS-Cache v2 hash/mscash2**). Результат сохраняется в реестр. Извлечь сами пароли пользователя или их хэши в открытом виде из реестра не получится. Поэтому если такой криптографический хэш попадет к злоумышленнику, ему придется выполнять перебор паролей с помощью брутфорса.

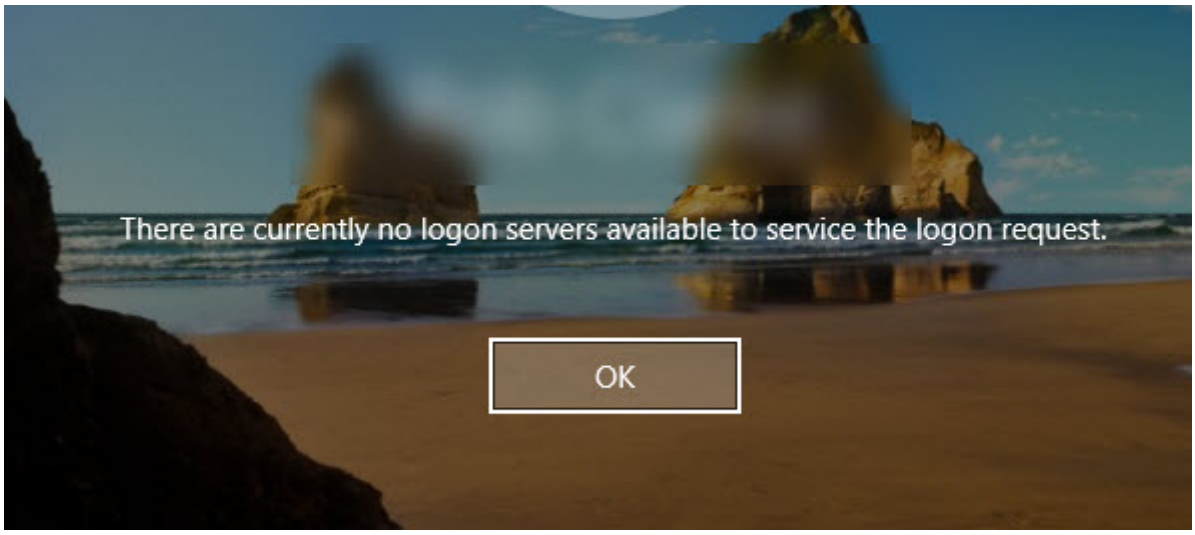
В реестре могут хранятся несколько хэшей доменных учетных записей, который входили на это компьютер ранее. По умолчанию сохраняются хэши десяти (**10**) последних пользователей.

Такой хэш хранится в реестре бессрочно (никогда не истекает, в отличии от доменных паролей), пока не будет перезатерт новым хэшем (когда пользователь входит на компьютер с новым паролем), или следующим пользователем (при превышении лимита хранимых кешей).

Если в локальном кэше для пользователя нет сохранённых учетных данных, то при входе на офлайн компьютер, появится сообщение:

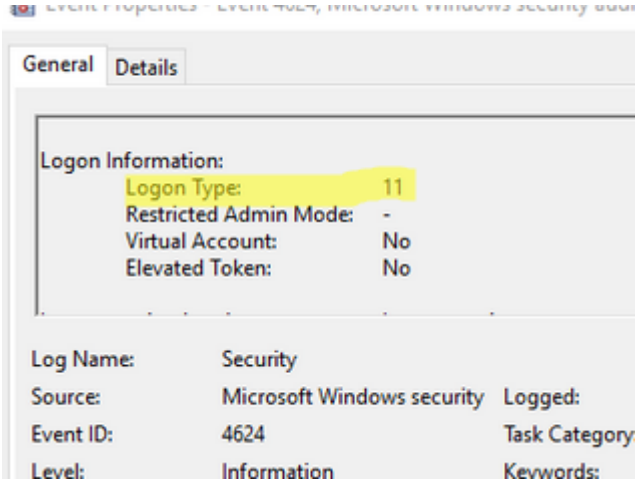
```
There are currently no logon servers available to service the logon request.
```

Отсутствуют серверы, которые могли бы обработать запрос на вход в сеть.



Когда пользователь входит на компьютер под кэшированными учетными данным, в журнале Security появится событие с **Event ID 4624** (An account was successfully logged on) и **Logon Type 11** (CachedInteractive). По таким событиям можно исследовать историю входов пользователей на компьютер Windows. Также возможны такие типа входов:

- **Logon Type 12**: CachedRemoteInteractive – удаленное подключение с использованием кэшированных учетных данных
- **Logon Type 13**: CachedUnlocked – разблокировка экрана компьютера после бездействия с помощью кэшированного пароля



Настройка Cached Credentials с помощью групповых политик

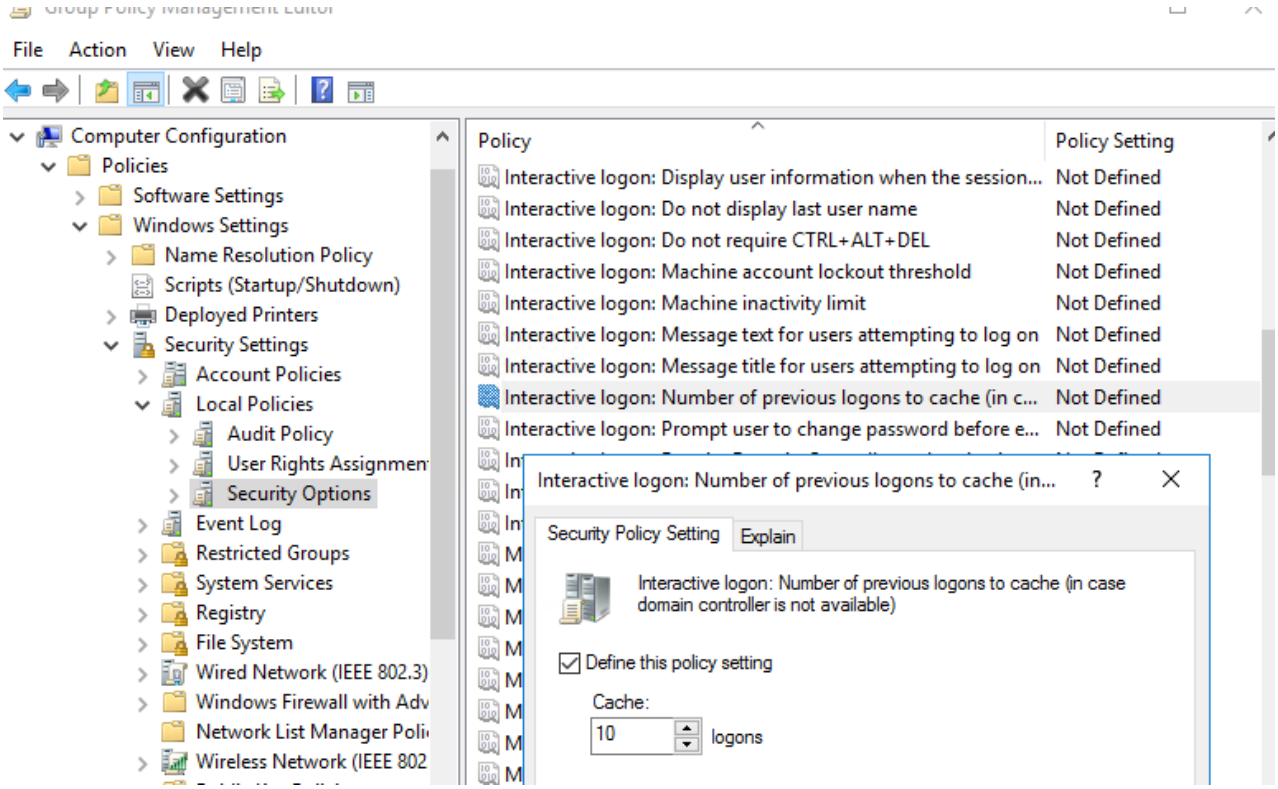
С помощью групповых политик можно настроить некоторые параметры кэширования учетных данных пользователей в Windows.

Изменить максимальное количество хранящийся кэшированных записей с учетными данными можно через параметр GPO. **logon: Number of previous logons to cache (in case domain controller is not available)** (Интерактивный вход в систему:

количество предыдущих подключений к кэшу в случае отсутствия доступа к контроллеру домена), который находится в разделе Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.

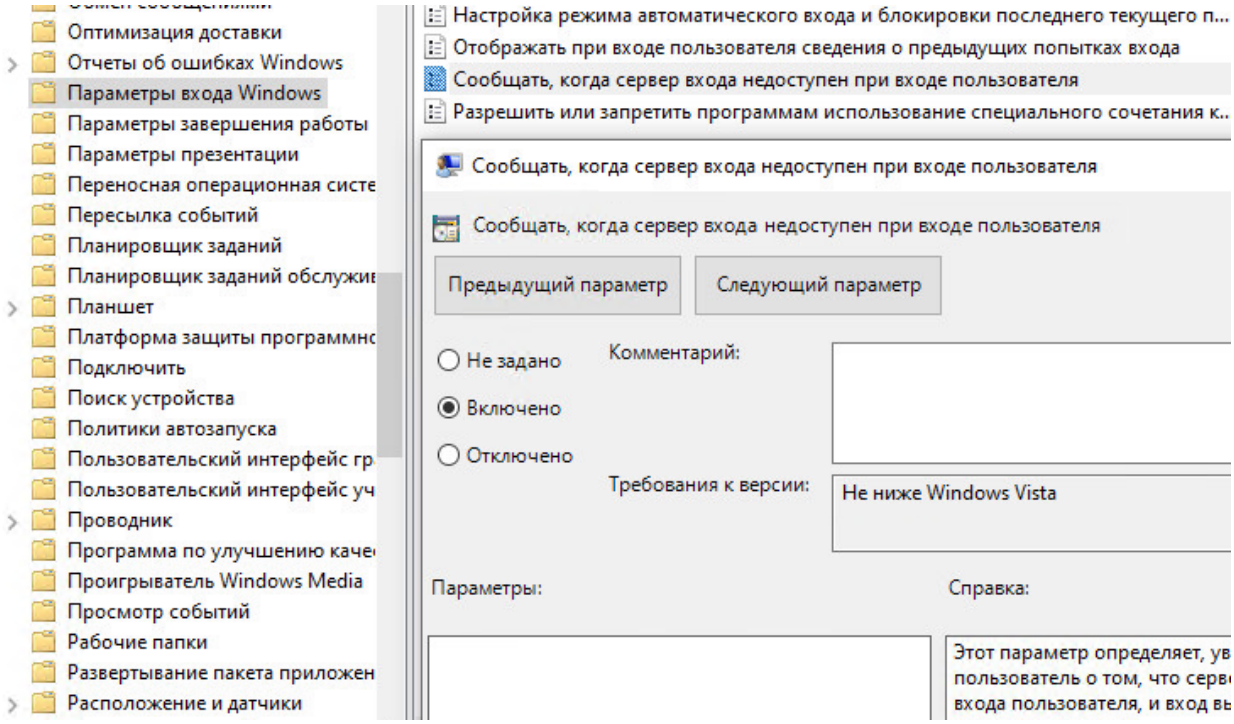
Значение по-умолчанию **10** (в реестре хранятся данные десяти последних вошедших на

Если задать **0**, это запретит Windows кэшировать учетные данные пользователей. В этом случае при недоступности домена, при входе пользователя появится ошибка “Отсутствуют серверы, которые могли бы обработать запрос на вход в сеть”.



Этот параметр также можно настроить с помощью REG_SZ параметра реестра **CashedLogonsCount из ветки** HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon.

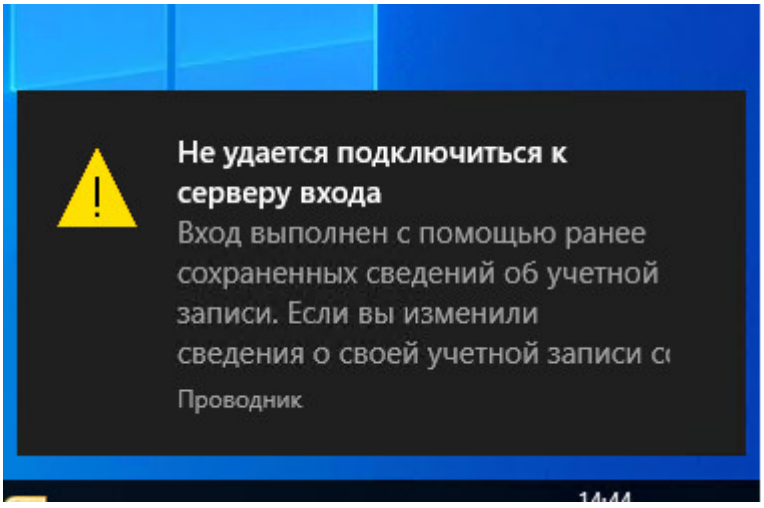
При входе под сохраненными данными, пользователь не видит, что контроллер домена не доступен. С помощью GPO можно вывести уведомление о входе под кэшированными данными. Для этого нужно включить политику **Report when logon server was not available during user logon** (Сообщать, когда сервер входа недоступен при входе пользователя) в разделе Computer configuration -> Policies -> Administrative templates -> Windows Components -> Windows Logon Options.



В этом случае при входе пользователя в трее будет появляться уведомление:

```
Не удается подключиться к серверу входа (контроллеру домена). Вход выполнен с помощью ранее сохраненных сведений об учетной записи.

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on might not be available.
```



Эту настройку можно включить через реестр:
HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/Current Version/Winlogon

- ValueName: ReportControllerMissing
- Data Type: REG_SZ
- Values: TRUE

Безопасность кэшированных учетных данных в Windows

Локальное кэширование данных аутентификации данных несет ряд рисков безопасности. Злоумышленник, получив физический доступ к компьютеру/ноутбуку с кэшированными данными, может с помощью брутфорса расшифровать хэш пароля (тут все зависит от сложности и длины пароля, для сложных паролей время подбора огромное). Поэтому не безопасно кешировать данные для входа учетных записей с правами локального администратора (или, тем более, доменного администратора).

Подробнее об обеспечении безопасности аккаунтов администраторов в сетях Windows.
Для уменьшения рисков безопасности, можно отключить кэширование учетных записей на офисных компьютерах и компьютерах администраторов. Для мобильных устройств желательно уменьшить количество кэшируемых аккаунтов до 1. Т.е. даже если администратор заходил на компьютер и его учетные данные попали в кэш, при входе пользователя-владельца устройства, хэш пароля администратора будет очищен.

Можно скрыть имя последнего вошедшего пользователя на экране входа в Windows.
Можно создать в домене отдельные политики по использованию кэшированных учетных данных для разных устройств и категорий пользователей (например, с помощью GPO Security filters, WMI фильтров, или распространению настроек параметра реестра CashedLogonsCount через GPP Item level targeting).

> Для мобильных пользователей – `CashedLogonsCount = 1`
> Для обычных компьютеров – `CashedLogonsCount = 0`

Такие политики снизят вероятность получения хэша привилегированных пользователей с персональных компьютеров.

Для защиты кэшированных данных на мобильных устройствах дополнительно можно включать шифрование системного диска BitLocker.

Можно добавить привилегированные учетные записи пользователей (администраторов) во встроенную доменную группу Protected Users (доступен для доменов с функциональным уровнем Windows Server 2012 R2 и выше). Для таких пользователей запрещено локальное сохранение кэшированных данных.

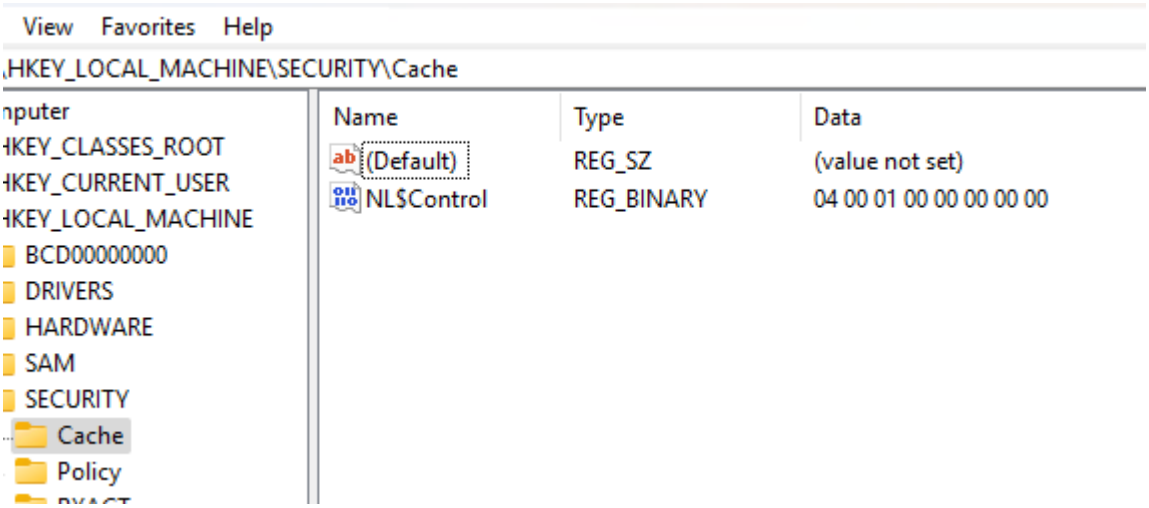
Если пользователи используют кешированный вход на компьютеры, а потом устанавливают VPN туннель в корпоративную сеть, они могут столкнуться с периодической блокировкой своей учетной записи в домене. Это будет происходить, если сохраненный локально пароль не соответствуеть паролю пользователя в домене (например, когда пользователь изменил его согласно настройкам политики паролей в домене). Для предотвращения такого сценария нужно настроить Windows, чтобы она запускала VPN туннель до входа пользователя в компьютер.

Очистка кэшированных учетных данных в Windows

Для очистки кэшированных данных для входа нужно удалить **NL$##** записи в реестре. Но делать это вручную не удобно, т.к. потребует запуска команды удаления от имени SYSTEM.

Если нужно очистить все сохраненные cashed credentials, нужно просто включить политику Interactive logon: Number of previous logons to cache (in case domain controller is not available) и задать значение **0** (описано выше).

После обновления настроек GPO командой `gpupdate /force` , информация кэшированные учетные данные в реестре будут удалены.



После этого можно отключить политику, или вернуть значение по умолчанию 10. После этого учетные данные всех последующих входов будут автоматически кэшироваться.