Диспетчер учетных данных Windows: управление сохраненными паролями

winitpro.ru/index.php/2012/04/17/upravlenie-soxranennymi-parolyami-v-windows-7

itpro

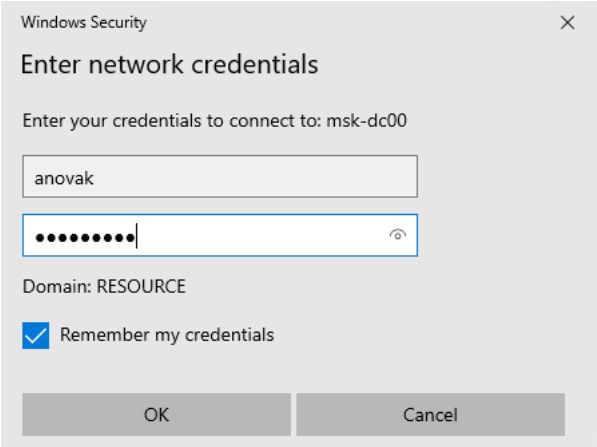
Диспетчер учетных данных Windows (Credential Manager) позволяет безопасно хранить учетные записи и пароля для доступа к сетевым ресурсам, веб сайтам и приложениям. Благодаря сохраненным в Credential Manager паролям вы можете подключаться без ввода пароля к сетевым ресурсам, которые поддерживаются проверку подлинности Windows (NTLM или Kerbersos), аутентификацию по сертификату, или базовую проверку подлинности.

Используем диспетчер учетных данных Windows для хранения паролей

Диспетчер учетных данных встроен в Windows и позволяет безопасно хранить три типа учетных данных:

- **Учетные данные Windows (Windows Credentials)** — учетные данные доступа к ресурсам, которые поддерживаются Windows аутентификацию (NTLM или Kerbersos). Это могут быть данные для подключения сетевых дисков или общим SMB папкам, NAS устройствам, сохраненные пароли для RDP подключений, пароли к сайтам, поддерживающих проверку подлинности Windows и т.д;
  Windows Credential не хранит данные для автоматического входа в Windows или доменные Cached Credentials.
- **Учетные данные сертификатов (Certificate-Based Credentials)** – используются для доступа к ресурсам с помощью сертификатов (из секции *Personal* в Certificate Manager);
- **Общие учетные данные (Generic Credentials)** – хранит учетные данные для доступа к сторонним приложениям, совместимым с Credential Manager и поддерживающим Basic аутентификацию;
- **Учетные данные для интернета (Web Credentials)** – сохранённые пароли в браузерах Edge и Internet Explorer, приложениях Microsoft (MS Office, Teams, Outlook, Skype и т.д).

Например, если при доступе к сетевой папке вы включите опцию “Сохранить пароль”, то введенный вами пароли будет сохранен в Credential Manager.

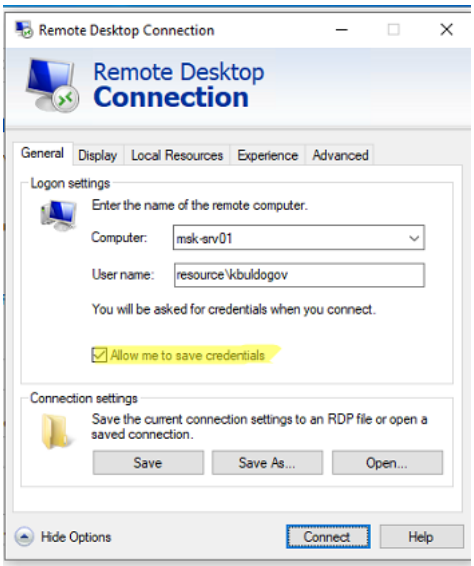


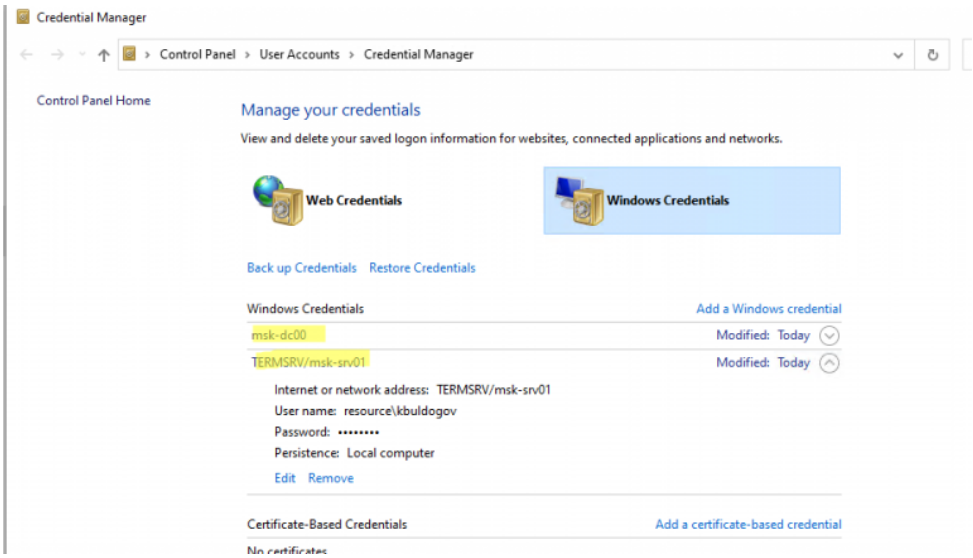
Аналогично пароль для подключения к удаленному RDP/RDS серверу сохраняется в клиенте Remote Desktop Connection (mstsc.exe).

Также в диспетчере паролей хранятся пароли пользователей, добавленные командой `runas /savecred` и используемые для запуска программ от имени другого пользователя.
Открыть диспетчер учетных данных в Windows можно:

- из классической панели управления (Control Panel\User Accounts\Credential Manager, Панель управления -> Учетные записи пользователей -> Диспетчер учетных данных);
- изкомандностроки: `control /name Microsoft.CredentialManager`

На скриншоте видно, что в Credential Manager хранятся два пароля, которые мы сохранили ранее.



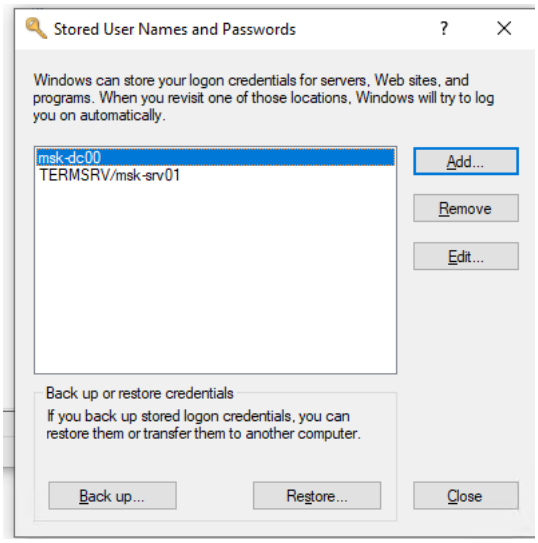


Сохраненный пароль для RDP подключения сохраняется в формате `TERMSRV\hostname` .

Здесь вы можете добавить сохранённый пароль, отредактировать (просмотреть сохраненный пароль в открытом виде из графического интерфейса нельзя) или удалить любую из записей.

Для управления сохраненными паролями можно использовать классический диалоговый интерфейс **Stored User Names and Password**. Для его запуска выполните команду:

```
rundll32.exe keymgr.dll,KRShowKeyMgr
```



Здесь вы также можете управлять сохраненными учетными данными, а также выполнить резервное копирование и восстановление записей в Credential Manager (можно использовать для переноса базы Credential Manager на другой компьютер).

Управление сохраненными учетными данными Windows из командной строки

Вы можете добавить удалить и вывести сохраненные учетные данных в Credentil Manager из командной строки с помощью утилиты **cmdkey**.

Добавить в диспетчер учетные данные для доступа к серверу FS01:

```
cmdkey /add:FS01 /user:kbuldogov /pass:Passw0rdd1
```

Если нужно сохранить доменную учетную запись:

```
cmdkey /add:fs01.winitpro.local /user:kbuldogov@winitpro.local /pass:Passw0rdd1
```

Сохранить учетные данные для доступа к RDP/RDS серверу:

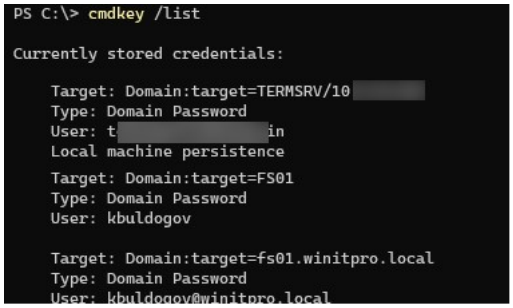
```
cmdkey /generic:termsrv/MSKRDS1 /user:kbuldogov /pass:Passw0rdd1
```

Для анонимного доступа к общей папке под гостевым аккаунтом, нужно добавить учетную запись guest без пароля:
```
cmdkey /add:192.168.13.200 /user:guest
```

Для удаленного управления гипервизором через консоль Hyper-V Manager, нужно сохранить пароль администраора Hyper-V:

```
cmdkey /add:hv19 /user:Administrator /pass:HVpas2ddr
```

Вывести список сохраненных учетных данных:
```
cmdkey /list
```



Вывести список хранимых учетных данных для указанного компьютера:
```
cmdkey /list:fs01.winitpro.local
```

Удалить ранее сохраненные учетные данные:

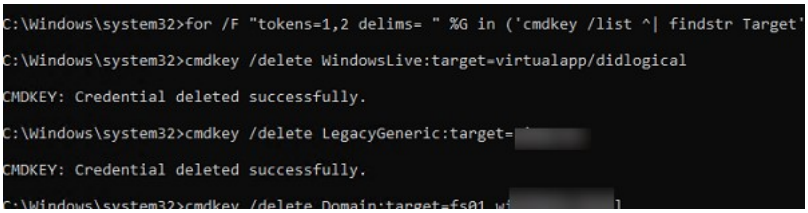
```
cmdkey /delete:FS01
```

Удалить из Credential Manager все сохраненные пароли для RDP доступа:

```
For /F "tokens=1,2 delims= " %G in ('cmdkey /list ^| findstr "target=TERMSRV"') do cmdkey /delete %H
```

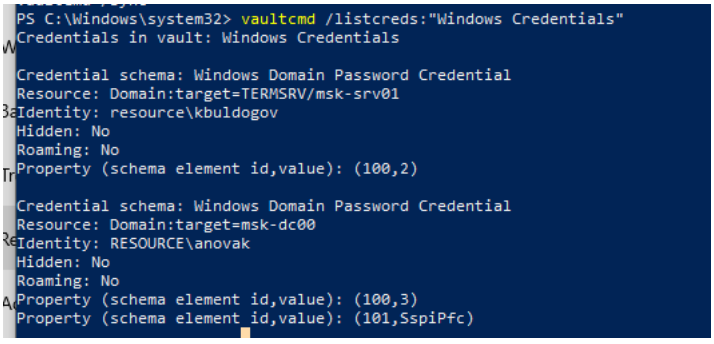
Полностью очистить пароли в Credential Manager:

```
for /F "tokens=1,2 delims= " %G in ('cmdkey /list ^| findstr Target') do cmdkey /delete %H
```



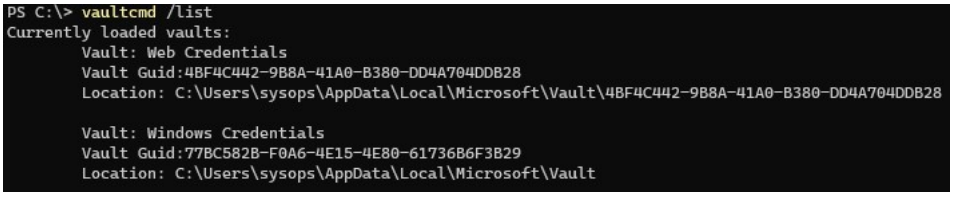
Эта команда позволяет быстро очистить старые сохраненные пароли, из за-которых может постоянно блокировать учетная запись пользователя в AD.
Также для управления сохраненными учетными данными можно использовать утилиту **vaultcmd**.Вывести список сохраненных учетных данных типа Windows Credentials:

```
vaultcmd /listcreds:"Windows Credentials"
```



Все сохраненные пароли хранятся в защищенном хранилище **Windows Vault**. Путь к хранилищу можно получить с помощью команды:

```
vaultcmd /list
```



По умолчанию это `%userprofile%\AppData\Local\Microsoft\Vault` . Ключ шифрования хранится в файле **Policy.vpol**. Клю шифровани используется для рашировки паролей в файлах **.vcrd**.

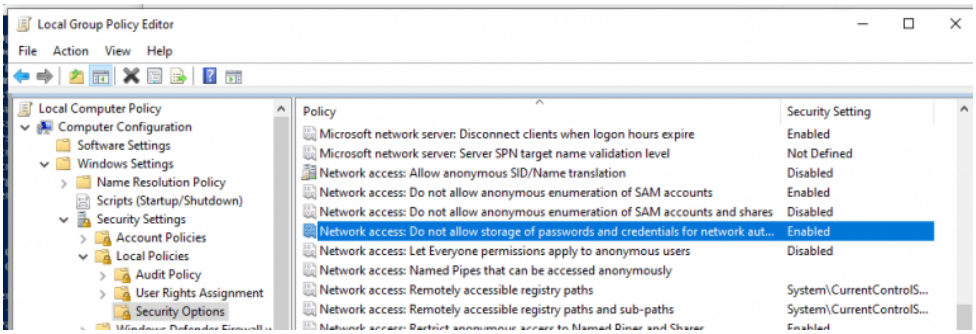
Для работы Credential Manager должна быть запущена служба **VaultSvc**:

```
Get-Service VaultSvc
```

Если служба отключена, при попытке получить доступ к Credential Manager появится ошибка:

```
Credential Manager Error
The Credential Manager Service is not running. You can start the service manually using the Services snap-in or restart your computer to start the service.
Error code: 0x800706B5
Error Message: The interface is unknown.
```

Если вы хотите заблокировать пользователям возможность сохранения сетевых паролей в Credential Manager, нужно включить параметр **Network access: Do not allow storage of passwords and credentials for network authentication** в разделе GPO Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.



Теперь, если пользователь попытается сохранить пароль в хранилище, появится ошибка:

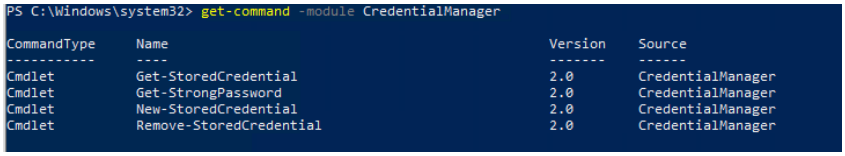
```
Credential Manager Error
Unable to save credentials. To save credentials in this vault, check your computer configuration.
Error code: 0x80070520
Error Message: A specified logon session does not exist. It may already have been terminated.
```

Доступ к менеджеру учетных данных Windows из PowerShell

В Windows нет встроенных командлетов для обращения к хранилищу PasswordVault из PowerShell. Но вы можете использовать модуль **CredentialManager** из галереи PowerShell.

Установите модуль:

```
Install-Module CredentialManager
```

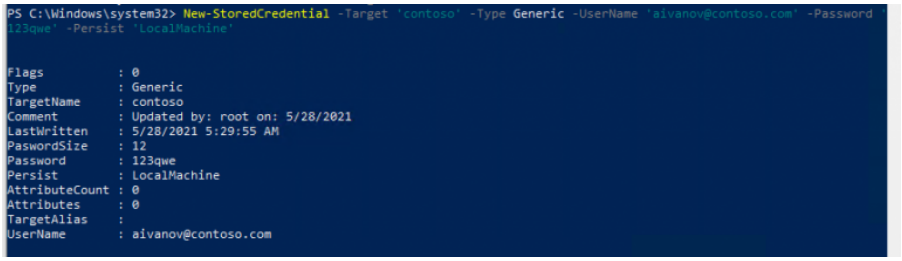


В модуле всего 4 командлета:

- Get-StoredCredential – получить учетные данные из хранилища Windows Vault;
- Get-StrongPassword – сгенерировать случайный пароль;
- New-StoredCredential – добавить учетные данные в хранилище;
- Remove-StoredCredential – удалить учетные данные.

Чтобы добавить новые учетные данные в хранилище CredentialManager, выполните команду:

```
New-StoredCredential -Target 'contoso' -Type Generic -UserName 'aivanov@contoso.com' -Password '123qwe' -Persist 'LocalMachine'
```



Проверить, есть в хранилище сохраненные данные:

```
Get-StoredCredential -Target contoso
```

С помощью командлета *Get-StoredCredential* вы можете вывести сохраненный пароль, хранящийся в диспетчере учетных данных в отрытом виде.

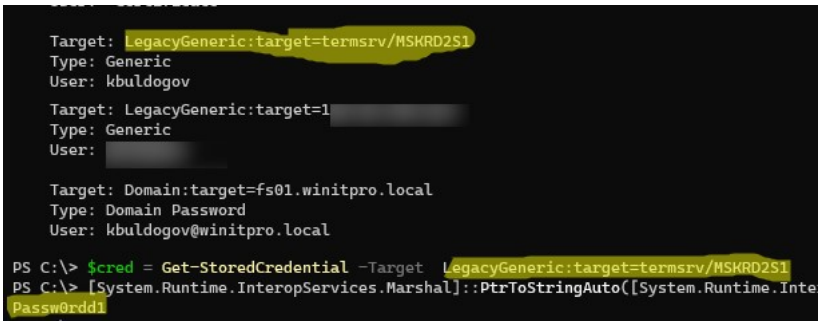
Выведите список сохраненных учетных данных:

```
cmdkey.exe /list
```

Скопируйте значение Target для объекта, пароль которого вы хотите извлечь и вставьте его в следующую команду:

```
$cred = Get-StoredCredential -Target  LegacyGeneric:target=termsrv/MSKRD2S1
[System.Runtime.InteropServices.Marshal]::PtrToStringAuto([System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($cred.Pa
```

Команда выведет сохраненный пароль в открытом виде.



Также для получения сохраненных паролей из credman в открытом виде можно использовать утилиты типа Mimikatz (смотри пример).
Сохраненные пароли из Credential Manager можно использовать в ваших скриптах PowerShell. Например, в следующем примере я получаю сохраненные имя и пароль в виде объекта PSCredential и подключаюсь с ними к Exchange Online из PowerShell:

```
$psCred = Get-StoredCredential -Target "Contoso"
Connect-MSolService -Credential $psCred
```

Также вы можете использовать Get-StoredCredential для безопасного получения сохранённых учетных данных в заданиях планировщика.

Также обратите внимание на модуль PowerShell Secret Management, который можно использовать для безопасного хранения паролей в Windows (поддерживает различные хранилища паролей: KeePass, LastPass, HashiCorp Vault, Azure Key Vault, Bitwarden.
Чтобы удалить сохраненные учетные данные из Windows Vault, выполните:

```
Remove-StoredCredential -Target Contoso
```

Комментариев: 16 Оставить комментарий

1. 

   Eugene 10.10.2019

   С помощью Powershell у далить кеш паролей в Windows 10 так

   ```
   $Credentials = (cmdkey /list | Where-Object {$_ -like "*Target=*"})
   Foreach ($Target in $Credentials) {
   $Target = ($Target -split (":", 2) | Select-Object -Skip 1).substring(1)
   $Argument = "/delete:" + $Target
   Start-Process Cmdkey -ArgumentList $Argument -NoNewWindow -RedirectStandardOutput $False
   }
   ```

   Ответить

2. 

   Елизавета 26.04.2021

   Это просто невыносимо-невозможно из-за рекламы ничего в Диспетчере паролей посмотреть.Ввожу запрос уже с десяток раз,а вижу одну рекламу.

   Ответить

3. **serg** 31.08.2022
Можно удалять пароли из диспетчере с помощьб cmdkey. Например вот так очищаются сохраненные rdp пароли

```
For /F "tokens=1,2 delims= " %G in ('cmdkey /list ^| findstr "target=TERMSRV"') do cmdkey /delete %H
```

Ответить

4. **Андрей** 05.07.2023
А есть ли возможность прописывать учетные данные на локальном компьютере так, чтобы они были доступны под сеансом другого пользователя? Или чтобы они были доступны для всех пользователей системы, а не только для того, под каким пользователем мы их добавляем?

Ответить

itpro 06.07.2023
Windows Credential хранит учетные данные в профиле каждого пользователя. Поэтому его использовать не получится. как вариант использовать внешнее хранлище секретов (например https://winitpro.ru/index.php/2021/05/11/modul-powershell-secret-management-hranenie-paroley/).
Или добавлять сораненные пароли для каждого пользователя (например, при входе логон скриптом):

```
cmdkey /add:TERMSRV/Server123 /user:winitpro\username /pass:Pa$$w0rd!
```

Ответить

- **Андрей** 06.07.2023
Спасибо за наводку по поводу выполнения скрипта при логоне.

  Ответить

- **Дмитрий** 21.02.2024
не работает

  Ответить

5. **Иван** 07.12.2023
vaultcmd /listcreds:»Windows Credentials» выдает «Недопустимое хранилище: элемент не найден»

Ответить

6. 

Александр 08.02.2024
Имеются доменные ПК (ноуты) win 10, сетевой диск win srv 2016.
Все в одном домене, аутентифицируются доменными учетными записями.
Юзерам примонтирован сетевой диск(через GPO), при физическом нахождении в офисе при открытии сетевого диска — получают доступ (без ввода пароля).
При подключении через VPN, вне офиса, при доступе к сетевому диску — открывается окно «Ввод учетных данных», причем в поле логин подставляется логин юзера от VPN подключения. Если ввести правильный доменный логин, пароль вручную, то после перезагрузки ПК — будет требовать ввода повторно. (пункт сохранить данные отмечается)
Почему так? как исправить?

Ответить

itpro 09.02.2024
Попробуйте настроить запуск VPN подключения до входа в Windows.
https://winitpro.ru/index.php/2013/06/16/zapusk-vpn-soedineniya-do-vxoda-v-sistemu-windows/
Подозреваю, что VPN пользователи входят под кэшированными учетными записиями и только после этого подключаются к VPN.

Ответить

Igor 14.10.2024
У меня такая же инфраструктура как у товарища выше. Независимо когда запускать ВПН, до входа в систему или после, когда пользователь находится вне офиса, так же выдает ошибку подключения. Лечится следующем образом: Панель управления\Учетные записи пользователей\Диспетчер учетных данных\Учетные данные Windows — Добавить учетные данные Windows. Вводятся имя файлового сервера, пользователь@domain.local, пароль, соответственно. После этого ресурсы доступны, все работает без нареканий.
Но, есть один нюанс — после перезагрузки ноута, эти учетные пропадают, надо все по новой прописать.
Есть идеи отчего не сохраняются на постоянку?

Ответить

itpro 17.10.2024
Сам по себе CredMan не должен очищать сохраненные пароли.
1) У вас пропадают только учетные данные, добавленные вручную или любые записи в диспетчере паролей?
2) Попробуйте добавить имя файлового сервера по FQDN и по короткому имени. Обе эти записи очищаются?
3) Вот нашел такое утверждение. Сам не проверял.

> If an entry does not exist for your CacheDrive and username, then Windows is not saving the login credentials. If an entry does appear but persistence is set to «Logon Session», then it will only be remembered until the next reboot.
> Credentials can also be verified at the command line using:
> cmdkey /list
> 2. If the Persistence setting is set to «Logon Session» and your computer is part of a domain, then try logging in with the following username format:
> $domain\$username

Ответить

7. **Михаил** 11.04.2024
После команды :
$cred = Get-StoredCredential -Target LegacyGeneric:target=termsrv/MSKRD2S1
[System.Runtime.InteropServices.Marshal]::PtrToStringAuto([System.Runtime.InteropServices.Marshal]::SecureStringToBSTR($cred.Pa

Выдает:
Исключение при вызове «SecureStringToBSTR» с «1» аргументами: «Значение не может быть неопределенным.
Имя параметра: s»
строка:2 знак:1
+ [System.Runtime.InteropServices.Marshal]::PtrToStringAuto([System.Run …
+ ~~~~~~
+ CategoryInfo : NotSpecified: (:) [], MethodInvocationException
+ FullyQualifiedErrorId : ArgumentNullException

что не так?

Ответить

itpro 12.04.2024
Переменная $cred случайно не пустая у вас?

Ответить

8. **Иван** 05.12.2024
А как можно удалить пароли другого пользователя, например, на другом компьютере через psexec.

Ответить

itpro 11.12.2024
cmdkey /list не позволяет видеть сохраненные пароли в профиле другого пользователя.
Только если запускать что-то от пользователя через runas или задание планировщика (можно раскидать на компьютеры через GPO).

Ответить