?????????? ?? ?????????? Active Directory

---

1. ???????????? ??????? ??????? ? ???????

1. ???????? ???????

Password Policy

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей -> Политика паролей
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

Описание:

Основа безопасности домена. Устанавливает минимальные требования к сложности, длине и сроку действия паролей пользователей.

Настройка:

- **Enforce password history:** Установить на `24` passwords remembered.
- **Maximum password age:** Установить на `60` days.
- **Minimum password length:** Установить на `12` characters или больше.
- **Password must meet complexity requirements:** `Enabled`. Требует наличия заглавных, строчных букв, цифр и спецсимволов.

Обоснование:

Предотвращает использование простых и легко подбираемых паролей, заставляет пользователей регулярно их менять, что значительно снижает риск несанкционированного доступа.

Пример команды PowerShell:

```
Set-ADDefaultDomainPasswordPolicy -ComplexityEnabled $true -MaxPasswordAge 60.00:00:00 -
MinPasswordLength 12 -PasswordHistoryCount 24
```

---

2. ???????? ?????????? ??????? ???????

Account Lockout Policy

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей -> Политика блокировки учетных записей
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy

Описание:

Автоматически блокирует учетную запись после нескольких неудачных попыток входа.

Настройка:

- **Account lockout threshold:** `5` invalid logon attempts.
- **Account lockout duration:** `15` minutes.
- **Reset account lockout counter after:** `15` minutes.

Обоснование:

Эффективная защита от атак методом подбора пароля (brute-force). Злоумышленник не сможет бесконечно перебирать пароли.

Пример команды PowerShell:

```
Set-ADDefaultDomainPasswordPolicy -LockoutDuration "0.00:15:00" -LockoutObservationWindow
"0.00:15:00" -LockoutThreshold 5
```

---

3. ??????????? ??????? ??????

Minimum password age

Путь в редакторе GPO:

```
```

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики учетных записей -> Политика паролей
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

Описание:

Устанавливает, сколько дней пользователь должен использовать пароль, прежде чем сможет его снова сменить.

Настройка:

Установить значение `1` day.

Обоснование:

Предотвращает ситуацию, когда пользователь, которого заставляют сменить пароль, меняет его и тут же меняет обратно на старый, обходя политику истории паролей.

Пример команды PowerShell:

```
Set-ADDefaultDomainPasswordPolicy -MinPasswordAge 1.00:00:00
```

---

4. ??????? ???????? ??????????? LAN Manager

LAN Manager authentication level

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Определяет, какой протокол аутентификации будет использоваться для сетевого входа.

Настройка:

Настроить политику `Network security: LAN Manager authentication level`, выбрав `Send NTLMv2 response only. Refuse LM & NTLM`.

Обоснование:

Устаревшие протоколы LM и NTLM уязвимы для атак. Принудительное использование NTLMv2 значительно повышает безопасность аутентификации в домене.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa" -Name "LmCompatibilityLevel" -Value 5
```

---

5. ?????? ???????? ????? LAN Manager

Do not store LAN Manager hash

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Запрещает системе хранить слабые, легко взламываемые LM-хеши паролей.

Настройка:

Включить (Enable) политику `Network security: Do not store LAN Manager hash value on next password change`.

Обоснование:

Критически важная политика безопасности. Даже если злоумышленник получит доступ к базе SAM или NTDS.dit, он не сможет извлечь из нее слабые LM-хеши для последующего взлома паролей.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa" -Name "NoLMHash" -
Value 1
```

---

6. ?? ?????????? ??? ?????????? ????????? ???????????

Do not display last signed-in

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Скрывает имя пользователя, который последним входил в систему, на экране входа.

Настройка:

Включить (Enable) политику `Interactive logon: Do not display last signed-in`.

Обоснование:

Повышает безопасность, так как потенциальному злоумышленнику потребуется знать не только пароль, но и имя пользователя для входа в систему.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"
-Name "DontDisplayLastUserName" -Value 1
```

---

7. ????????? ????????? ??? ???????? ?????-?????

Smart card removal behavior

Путь в редакторе GPO:

>

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Определяет, что произойдет, когда пользователь извлекает смарт-карту из считывателя.

Настройка:

Настроить политику `Interactive logon: Smart card removal behavior`, выбрав `Lock Workstation`.

Обоснование:

Критически важная политика для сред с двухфакторной аутентификацией. Гарантирует, что рабочая станция будет немедленно заблокирована, как только физический токен (смарт-карта) будет удален.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon" -Name "scremoveoption" -Value "1"
```

---

8. ????????? ??????????? ??????? ??????

Number of previous logons to cache

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Запрещает системе кешировать учетные данные для входа в домен. Вход будет возможен только при доступности контроллера домена.

Настройка:

Настроить политику `Interactive logon: Number of previous logons to cache (in case domain controller is not available)`, установив значение `0`.

Обоснование:

Максимальный уровень безопасности для стационарных рабочих станций. Предотвращает возможность входа в систему с использованием старого (потенциально скомпрометированного) пароля, если компьютер отключен от сети.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon" -Name "CachedLogonsCount" -Value 0
```

---

9. ????????? ?????? LSA

Enable LSA Protection

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Система -> Local Security Authority
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> System -> Local Security Authority

Описание:

Защищает процесс Local Security Authority (LSA) от внедрения кода, что усложняет кражу учетных данных из памяти.

Настройка:

Включить (Enable) политику `Configure LSASS to run as a protected process` и установить значение `Enabled with UEFI Lock`.

Обоснование:

Значительно повышает устойчивость системы к современным атакам, таким как Mimikatz, которые нацелены на извлечение паролей и хэшей из памяти процесса LSASS.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa" -Name "RunAsPPL" -
Value 1
```

---

2. ??????????? ??????? ? ???????????

10. ?????? ??????? ? ?????? ??????????? ? ???????????

Prohibit access to Control Panel and PC settings

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Панель управления
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Control Panel

Описание:

Полностью блокирует доступ пользователей к классической Панели управления и современному приложению "Параметры".

Настройка:

Найти и включить (Enable) политику `Prohibit access to Control Panel and PC settings`.

Обоснование:

Критически важная политика для ограничения прав пользователей. Предотвращает несанкционированные изменения в конфигурации системы, установку/удаление программ и изменение сетевых настроек.

Пример команды PowerShell:

```
# This is a user policy, applied on logon.
# To set via registry for the current user:
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name
```

```
"NoControlPanel" -Value 1
```

---

11. ?????? ?? ????????????? ??????? ?????????

Restrict Removable Storage Access

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Система -> Доступ к съемным запоминающим устройствам
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> System -> Removable Storage Access

Описание:

Контролирует доступ к USB-накопителям, внешним дискам, CD/DVD и другим съемным устройствам.

Настройка:

Включить (Enable) политику `All Removable Storage classes: Deny all access` для полной блокировки. Можно настроить более гранулярно, например, разрешить только чтение.

Обоснование:

Ключевой элемент предотвращения утечек данных (DLP) и защиты от вредоносного ПО, распространяемого через USB-флешки.

Пример команды PowerShell:

```
# This policy controls multiple registry keys.
# Example to deny write access to USB storage:
Set-ItemProperty -Path
"HKLM:\\Software\\Policies\\Microsoft\\Windows\\RemovableStorageDevices\\{53f5630d-b6bf-11d0-
94f2-00a0c91efb8b}" -Name "Deny_Write" -Value 1
```

---

12. AppLocker / ???????? ????????????? ????????????? ????????

AppLocker / Software Restriction Policies

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Политики управления приложениями -> AppLocker
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Application Control Policies -> AppLocker

Описание:

Позволяет создать "белый список" приложений, разрешенных к запуску. Все остальное будет заблокировано.

Настройка:

Сначала необходимо создать правила по умолчанию (ПКМ → Create Default Rules). Затем можно создавать свои правила для исполняемых файлов (Executable Rules) на основе пути, хэша файла или издателя.

Не забудьте запустить службу `Application Identity` (`gpsvc`) на клиентских машинах для применения политик.

Обоснование:

Одна из самых надежных защит от вирусов и программ-шифровальщиков. Даже если пользователь скачает вредоносный файл, он просто не сможет его запустить.

Пример команды PowerShell:

```
# AppLocker policies are complex XML files. Managing them via PowerShell is advanced.
# Example to get the current policy:
Get-AppLockerPolicy -Local | Export-Clixml -Path C:\\AppLocker.xml
```

---

13. ?????? ??????? ? ????????? ??????

Prevent access to the command prompt

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Система
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> System

Описание:

Отключает доступ к командной строке (cmd.exe) для пользователей.

Настройка:

Найти и включить (Enable) политику `Prevent access to the command prompt`. Можно также запретить выполнение скриптов.

Обоснование:

Сильная мера безопасности для сред с повышенными требованиями, где пользователям не должно быть разрешено выполнять системные команды.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKCU:\\Software\\Policies\\Microsoft\\Windows\\System" -Name "DisableCMD" -Value 1
```

---

14. ?????????? "???????????????? ?????"

Turn off Microsoft consumer experiences

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Содержимое из облака
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Cloud Content

Описание:

Отключает загрузку и установку рекламируемых приложений (Candy Crush, Spotify и т.п.) в Windows 10/11 Pro.

Настройка:

Найти и включить (Enable) политику `Turn off Microsoft consumer experiences`.

Обоснование:

Убирает ненужное ПО с корпоративных рабочих мест, сохраняя "чистоту" системы и экономя место на диске.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows\\CloudContent" -Name "DisableWindowsConsumerFeatures" -Value 1
```

---

15. ????????? ?????????? ??? ???? ??????

Turn off Autoplay

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Политики автозапуска
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> AutoPlay Policies

Описание:

Полностью отключает функцию автозапуска/автовоспроизведения для всех типов дисков.

Настройка:

Включить (Enable) политику `Turn off Autoplay` и выбрать опцию `All drives`.

Обоснование:

Исторически, автозапуск был одним из главных векторов распространения вирусов через USB-накопители. Отключение этой функции является важным шагом для повышения безопасности рабочих станций.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name "NoDriveTypeAutoRun" -Value 255
```

---

16. ????????? ?????? ? ???????

Prevent access to registry editing tools

Путь в редакторе GPO:

>

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Система
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> System

Описание:

Блокирует запуск редактора реестра (`regedit.exe`).

Настройка:

Включить (Enable) политику `Prevent access to registry editing tools`.

Обоснование:

Предотвращает ручное изменение критически важных системных настроек пользователями, что может привести к нестабильной работе или полному отказу системы.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System" -Name "DisableRegistryTools" -Value 1
```

---

17. ????????? ?????? ????????? ??????????

Don't run specified Windows applications

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Система
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> System

Описание:

Создает "черный список" приложений, которые пользователям запрещено запускать.

Настройка:

Включить (Enable) политику, нажать `Show...` и добавить имена исполняемых файлов (например, `bittorrent.exe`).

Обоснование:

Более простой способ блокировки приложений по сравнению с AppLocker. Подходит для быстрого запрета нежелательного ПО (торрент-клиенты, игры и т.д.).

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\DisallowRun" -Name
"1" -Value "bittorrent.exe"
```

---

18. ????????? ????????? UAC

Configure User Account Control (UAC)

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Управляет поведением контроля учетных записей (UAC).

Настройка:

Найти и настроить политику `User Account Control: Behavior of the elevation prompt for administrators...`. Например, установить `Prompt for consent for non-Windows binaries`.

Обоснование:

Позволяет найти баланс между безопасностью и удобством, настраивая, как часто и для каких действий система будет запрашивать подтверждение с повышенными привилегиями.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"
-Name "ConsentPromptBehaviorAdmin" -Value 5
```

---

3. ??????? ???? ? ????? ???????????

19. ?????????? ??????? ??????

Map Network Drives

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Настройка -> Конфигурация Windows -> Сопоставления дисков
>
> **EN:** User Configuration -> Preferences -> Windows Settings -> Drive Maps

Описание:

Автоматически подключает сетевые папки в качестве дисков при входе пользователя в систему.

Настройка:

Внутри GPO, в указанном пути:

1. ПКМ → New → Mapped Drive.
2. **Action:** `Update` (создает или обновляет диск).
3. **Location:** `\\server\share\folder` (путь к сетевой папке).
4. **Reconnect:** Отметить галочкой.
5. **Label as:** Понятное имя диска (например, "Общие документы").
6. **Drive Letter:** Выбрать букву диска.

Обоснование:

Стандартизирует рабочее окружение, обеспечивает легкий и единообразный доступ к общим ресурсам, избавляя пользователей от необходимости подключать диски вручную.

Пример команды PowerShell:

```
# Drive Maps через GPO Preferences не имеют прямого командлета.
# Пример подключения диска для текущего сеанса:
New-PSDrive -Name "S" -PSProvider "FileSystem" -Root "\\\\server\\share" -Persist
```

---

20. ????????? ????? ???????? ?????

Desktop Wallpaper

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Рабочий стол -> Рабочий стол
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Desktop -> Desktop

Описание:

Принудительно устанавливает единые обои рабочего стола для всех пользователей.

Настройка:

Включить (Enable) политику **Desktop Wallpaper** и указать UNC-путь к файлу изображения в поле `Wallpaper Name`. Например: `\\server\share\wallpapers\corporate.jpg`.

Убедитесь, что у всех пользователей есть права на чтение этого файла.

Обоснование:

Обеспечивает корпоративный брендинг, поддерживает профессиональный вид рабочих станций и предотвращает установку неуместных или отвлекающих изображений.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"
-Name "Wallpaper" -Value "\\\\server\\share\\wallpapers\\corporate.jpg"
```

---

21. ?????? ?? ????????? ???????? ?????

Prevent changing desktop background

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Панель управления -> Персонализация
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Control Panel -> Personalization

Описание:

Запрещает пользователям изменять обои рабочего стола.

Настройка:

Включить (Enable) политику `Prevent changing desktop background`. Работает в паре с политикой принудительной установки обоев.

Обоснование:

Поддерживает корпоративный стандарт и предотвращает установку неуместных или отвлекающих изображений, дополняя политику принудительной установки обоев.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\ActiveDesktop" -Name
"NoChangingWallPaper" -Value 1
```

---

22. ?????????????? ?????

Folder Redirection

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Конфигурация Windows -> Перенаправление папок
>
> **EN:** User Configuration -> Policies -> Windows Settings -> Folder Redirection

Описание:

Перенаправляет стандартные папки пользователя (Документы, Рабочий стол и т.д.) на сетевой ресурс.

Настройка:

ПКМ на папке (например, `Documents`) → Properties.

- **Setting:** `Basic - Redirect everyone's folder to the same location`.
- **Target folder location:** `Create a folder for each user under the root path`.
- **Root Path:** `\\server\profiles\%USERNAME%\Documents`.

Обоснование:

Централизует хранение пользовательских данных, что упрощает их резервное копирование. Также обеспечивает "бесшовный" переход пользователя между разными компьютерами в домене — его файлы всегда с ним.

Пример команды PowerShell:

```
# Folder Redirection не имеет прямого командлета и настраивается через GUI.
```

---

23. ?????? ????????? ?????/??????

Logon/Logoff Scripts

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Конфигурация Windows -> Сценарии (вход/выход из системы)
>
> **EN:** User Configuration -> Policies -> Windows Settings -> Scripts (Logon/Logoff)

Описание:

Выполняет скрипты (.bat, .vbs, .ps1) при входе пользователя в систему или выходе из нее.

Настройка:

Двойной клик по `Logon`, на вкладке `PowerShell Scripts` нажать `Add...` и указать путь к скрипту. Скрипты должны храниться в папке политики на контроллере домена (Sysvol).

Обоснование:

Мощный инструмент автоматизации для задач, которые нужно выполнять для каждого пользователя: подключение принтеров, создание ярлыков, очистка временных файлов.

Пример команды PowerShell:

```
Set-GPRegistryValue -Name "MyGPO" -Key
"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Group Policy\\Scripts\\Logon\\0" -
ValueName "Script" -Value "\\\\domain.com\\SysVol\\...\\MyScript.ps1" -Type String
```

---

24. ????????? ??? ????? ? ???????

Interactive logon message

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options

Описание:

Отображает юридическое или информационное сообщение перед входом пользователя в систему.

Настройка:

Настроить две политики:

- **Interactive logon: Message text for users...** (Текст сообщения, например, "Этот компьютер является собственностью компании...").
- **Interactive logon: Message title for users...** (Заголовок окна сообщения, например, "ПРЕДУПРЕЖДЕНИЕ").

Обоснование:

Используется для юридических уведомлений об ответственности за использование корпоративных ресурсов и для информирования пользователей о плановых работах.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"
-Name "legalnoticecaption" -Value "ПРЕДУПРЕЖДЕНИЕ"
Set-ItemProperty -Path "HKLM:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System"
-Name "legalnoticetext" -Value "Этот компьютер является собственностью компании."
```

---

25. ????????? ?????????? ?????? ? ???????

Enable Screen Saver Password Protection

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Панель управления -> Персонализация
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Control Panel -> Personalization

Описание:

Принудительно включает заставку и требует ввод пароля для разблокировки компьютера.

Настройка:

- Включить **Password protect the screen saver**.
- Включить **Screen saver timeout** и установить время в секундах (например, `600` для 10 минут).
- Включить **Force specific screen saver** и указать путь к файлу (например, `scrnsave.scr`).

Обоснование:

Обеспечивает безопасность рабочих станций, оставленных без присмотра. Если пользователь отошел, компьютер автоматически заблокируется.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKCU:\\Software\\Policies\\Microsoft\\Windows\\Control Panel\\Desktop" -Name "ScreenSaveActive" -Value "1"
Set-ItemProperty -Path "HKCU:\\Software\\Policies\\Microsoft\\Windows\\Control Panel\\Desktop" -Name "ScreenSaverIsSecure" -Value "1"
Set-ItemProperty -Path "HKCU:\\Software\\Policies\\Microsoft\\Windows\\Control Panel\\Desktop" -Name "ScreenSaveTimeOut" -Value "600"
```

---

26. ?????? ????????? ?????

Hide these specified drives in My Computer

Путь в редакторе GPO:

>

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Компоненты Windows -> Проводник
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Windows Components -> File Explorer

Описание:

Скрывает определенные диски (например, системный диск C:) из окна "Этот компьютер".

Настройка:

Включить (Enable) политику и выбрать из выпадающего списка комбинацию дисков, которые нужно скрыть.

Обоснование:

Используется для упрощения интерфейса для пользователя, скрывая системные разделы, которые ему не нужно трогать, и оставляя только диски с данными.

Пример команды PowerShell:

```
# Hides drive C. The value is a bitmask. 4 corresponds to C.
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name "NoDrives" -
Value 4
```

---

27. ?????? ?????????????? ???????????? ??????? ?????

Remove "Map Network Drive" and "Disconnect Network Drive"

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Компоненты Windows -> Проводник
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Windows Components -> File Explorer

Описание:

Убирает из интерфейса Проводника пункты "Подключить сетевой диск" и "Отключить сетевой диск".

Настройка:

Включить (Enable) политику `Remove "Map Network Drive" and "Disconnect Network Drive"`.

Обоснование:

Позволяет полностью контролировать подключение сетевых дисков через GPO, запрещая пользователям самостоятельно подключать или отключать другие сетевые ресурсы.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name
"NoNetConnectDisconnect" -Value 1
```

---

28. ????????? ?????? ? ????????? ????? ??????????

Removes the "Properties" item from the This PC context menu

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Компоненты Windows -> Проводник
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Windows Components -> File Explorer

Описание:

Удаляет пункт "Свойства" из контекстного меню значка "Этот компьютер".

Настройка:

Включить (Enable) политику `Removes the "Properties" item from the This PC context menu`.

Обоснование:

Ограничивает возможность пользователя просматривать основную информацию о системе, изменять имя компьютера, рабочую группу или домен, что является частью общей стратегии по ограничению прав.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name
"NoPropertiesMyComputer" -Value 1
```

---

29. ?? ????????? ???????? ?????????

Do not keep history of recently opened documents

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Компоненты Windows -> Проводник
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Windows Components -> File Explorer

Описание:

Отключает ведение истории недавно открытых файлов.

Настройка:

Включить (Enable) политику `Do not keep history of recently opened documents`.

Обоснование:

Повышает конфиденциальность, особенно на компьютерах с общим доступом, так как другие пользователи не смогут увидеть, какие документы открывались ранее.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name
"NoRecentDocsHistory" -Value 1
```

---

4. ???????????? ?????????? ??????? (RDP)

30. ????????? ????????? ??????????? ?? RDP

Allow users to connect remotely by using Remote Desktop Services

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов -> Узел сеансов удаленных рабочих столов -> Подключения
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Connections

Описание:

Главный переключатель, разрешающий или запрещающий RDP-подключения к серверу.

Настройка:

Включить (Enable) политику. Чтобы запретить RDP, установите в "Отключено" (Disabled).

Обоснование:

Позволяет централизованно управлять доступностью RDP на множестве компьютеров. Является основой для всех остальных настроек RDP.

Пример команды PowerShell:

```
# To enable RDP:
Set-ItemProperty -Path 'HKLM:\\System\\CurrentControlSet\\Control\\Terminal Server' -name
"fDenyTSConnections" -value 0
#To disable RDP:
Set-ItemProperty -Path 'HKLM:\\System\\CurrentControlSet\\Control\\Terminal Server' -name
"fDenyTSConnections" -value 1
```

---

31. ?????????? ????????????? ? ?????? "???????????? ?????????? ???????? ?????"

Allow log on through Remote Desktop Services

Путь в редакторе GPO:

>

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Назначение прав пользователя
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment

Описание:

Определяет, какие пользователи или группы могут подключаться к компьютеру по RDP.

Настройка:

Открыть политику, нажать "Добавить пользователя или группу..." и указать доменную группу, членам которой будет разрешен RDP-доступ (например, `DOMAIN\RemoteUsers`).

Обоснование:

Правильный способ управления доступом по RDP. Вместо добавления пользователей в локальную группу "Пользователи удаленного рабочего стола" вручную, вы централизованно управляете членством в доменной группе.

Пример команды PowerShell:

```
# This policy configures a security identifier (SID) and is best managed via the GPO GUI.
```

---

32. ????????? ???????? ??????????? ?? ?????? ???? (NLA)

Require user authentication for remote connections by using Network Level Authentication

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов -> Узел сеансов удаленных рабочих столов -> Безопасность
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security

Описание:

Требует, чтобы пользователь прошел аутентификацию до установления полноценного сеанса RDP.

Настройка:

Включить (Enable) политику.

Обоснование:

Ключевая мера безопасности RDP. Защищает от DoS-атак и использования уязвимостей в протоколе до аутентификации (например, BlueKeep). Сессия не будет создана, пока пользователь не подтвердит свою личность.

Пример команды PowerShell:

```
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace
root\\cimv2\\terminalservices).SetUserAuthenticationRequired(1)
```

---

33. ?????????? ??????? ?????????? ??????????? ???????????

Set client connection encryption level

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов -> Узел сеансов удаленных рабочих столов -> Безопасность
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Security

Описание:

Задает минимальный уровень шифрования для RDP-сеансов.

Настройка:

Включить (Enable) политику и в выпадающем списке выбрать `High Level`.

Обоснование:

Гарантирует, что для всех RDP-соединений используется надежное 128-битное шифрование, защищая передаваемый трафик от перехвата и анализа.

Пример команды PowerShell:

```
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace
root\\cimv2\\terminalservices).MinEncryptionLevel = 3
```

---

34. ????????? ?????????? ??????? RDP

Do not allow passwords to be saved

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов -> Клиент подключения к удаленному рабочему столу
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Connection Client

Описание:

Отключает на клиентских машинах возможность сохранения паролей в RDP-клиенте (деактивирует галочку "Запомнить меня").

Настройка:

Включить (Enable) политику. Эта политика применяется к компьютерам, с которых производятся подключения.

Обоснование:

Предотвращает хранение паролей на рабочих станциях, что является критически важным для безопасности, особенно на компьютерах с общим доступом, и снижает риск компрометации учетных данных.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows NT\\Terminal Services" -
Name "DisablePasswordSaving" -Value 1
```

---

35. ?????? ??????????? ?????? ??? ???????????

Prompt for credentials on the client computer

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов -> Клиент подключения к удаленному рабочему столу
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Connection Client

Описание:

Заставляет RDP-клиент всегда запрашивать пароль, даже если он был сохранен ранее.

Настройка:

Включить (Enable) политику. Эта политика также применяется к клиентским машинам.

Обоснование:

Повышает безопасность, требуя от пользователя активного ввода пароля при каждом подключении, что снижает риск использования скомпрометированных сохраненных учетных данных.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows NT\\Terminal Services" -Name "PromptForCredentials" -Value 1
```

---

36. ????? ???????? ????? ??????????? ?????? RDP

Set time limit for active but idle Remote Desktop Services sessions

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Службы удаленных рабочих столов ->

> Узел сеансов удаленных рабочих столов -> Ограничения по времени для сеансов
>
> **EN:** Computer Configuration -> ... -> Remote Desktop Services -> Remote Desktop Session Host -> Session Time Limits

Описание:

Автоматически отключает неактивные (простаивающие) сеансы на сервере терминалов.

Настройка:

Включить (Enable) политику и установить лимит, например, `1 hour`.

Обоснование:

Освобождает лицензии и системные ресурсы на RDS-ферме от пользователей, которые подключились и забыли выйти, повышая эффективность использования сервера.

Пример команды PowerShell:

```
# This policy corresponds to a registry key. 3600000 milliseconds = 1 hour.
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows NT\\Terminal Services" -Name "MaxIdleTime" -Value 3600000
```

---

37. ??????? ???? "?????????? ??????" ?? ?????? RDP

Remove and prevent access to the Shut Down command

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Политики -> Административные шаблоны -> Меню "Пуск" и панель задач
>
> **EN:** User Configuration -> Policies -> Administrative Templates -> Start Menu and Taskbar

Описание:

Убирает из меню "Пуск" кнопки выключения, перезагрузки и сна. Особенно полезно для серверов терминалов.

Настройка:

Включить (Enable) политику `Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands`.

Обоснование:

Предотвращает случайное или намеренное выключение или перезагрузку критически важных серверов (например, RDS-ферм) обычными пользователями.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer" -Name "NoClose" -
Value 1
```

---

5. ????? ? ??????????? ????????????

38. ????? ??????? ????? ? ???????

Audit logon events

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Политика аудита
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy

Описание:

Включает запись в журнал безопасности событий успешного и неуспешного входа в систему.

Настройка:

Найти политику `Audit logon events` и включить аудит для `Success` и `Failure`.

Обоснование:

Критически важно для расследования инцидентов безопасности. Позволяет отслеживать, кто, когда и с какого компьютера пытался войти в систему.

Пример команды PowerShell:

```
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
```

---

39. ????? ??????? ? ????????

Audit object access

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Политика аудита
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy

Описание:

Включает аудит доступа к файлам, папкам и объектам реестра.

Настройка:

Включить политику `Audit object access` для `Success` и `Failure`. После этого необходимо настроить аудит на конкретных папках (вкладка "Безопасность" → "Дополнительно" → "Аудит").

Обоснование:

Позволяет отслеживать, кто и когда получал доступ к критически важным файлам, изменял или удалял их. Необходимо для расследования инцидентов и соответствия стандартам безопасности.

Пример команды PowerShell:

```
auditpol /set /category:"Object Access" /success:enable /failure:enable
```

---

40. ????????? ??????? ??????? ????????? PowerShell

Turn on PowerShell Script Block Logging

Путь в редакторе GPO:

>

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Windows PowerShell
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell

Описание:

Включает детальное логирование всех блоков кода PowerShell, которые выполняются в системе.

Настройка:

Включить (Enable) политику `Turn on PowerShell Script Block Logging`. События будут записываться в журнал `Microsoft-Windows-PowerShell/Operational`.

Обоснование:

Критически важный инструмент для обнаружения вредоносной активности. Так как многие современные атаки используют PowerShell, эта политика позволяет видеть точные команды, которые выполнял злоумышленник.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKLM:\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\ScriptBlockLogging" -Name
"EnableScriptBlockLogging" -Value 1
```

---

41. ???????? ???????????? PowerShell

Turn on PowerShell Transcription

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Windows PowerShell
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell

Описание:

Записывает весь ввод и вывод из консоли PowerShell в текстовые файлы.

Настройка:

Включить (Enable) политику и указать сетевую папку (UNC-путь), куда будут сохраняться логи. Это дополняет политику ведения журнала блоков.

Обоснование:

Создает полный, человеко-читаемый протокол всего, что происходило в сессиях PowerShell. Бесценно для анализа сложных атак и действий администраторов.

Пример команды PowerShell:

```
Set-ItemProperty -Path
"HKLM:\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\Transcription" -Name
"EnableTranscripting" -Value 1
Set-ItemProperty -Path
"HKLM:\\Software\\Policies\\Microsoft\\Windows\\PowerShell\\Transcription" -Name
"OutputDirectory" -Value "\\\\server\\share\\PSTranscripts"
```

---

42. ????? ????????? ????????

Audit policy change

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Политика аудита
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy

Описание:

Включает аудит изменений в политиках назначения прав, аудита и доверительных отношений.

Настройка:

Включить политику `Audit policy change` для `Success` и `Failure`.

Обоснование:

Помогает отслеживать, не пытается ли злоумышленник или недобросовестный администратор изменить политики безопасности, чтобы скрыть свои следы или получить несанкционированные привилегии.

Пример команды PowerShell:

```
auditpol /set /category:"Policy Change" /success:enable /failure:enable
```

---

43. ???????? ??????????? ?????

Force audit policy subcategory settings

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Локальные политики -> Параметры безопасности
>
> **EN:** Computer Configuration -> Policies -> Windows Settings -> Local Policies -> Security Options

Описание:

Принудительно использует новые, более гранулярные настройки расширенного аудита, игнорируя старые базовые политики.

Настройка:

Включить (Enable) политику `Audit: Force audit policy subcategory settings...`. Это позволяет тонко настраивать аудит в разделе `Advanced Audit Policy Configuration`.

Обоснование:

Современный подход к аудиту. Вместо одной общей политики "Audit object access" можно включить аудит отдельно для файловой системы, реестра, SAM и т.д., что уменьшает "шум" в журналах безопасности.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa" -Name
"SCENoApplyLegacyAuditPolicy" -Value 1
```

---

6. ???????????? ? ?????????? ????????

44. ????????? ?? ????? GPO

Software Installation via GPO

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация программ -> Установка программ
>
> **EN:** Computer Configuration -> Policies -> Software Settings -> Software installation

Описание:

Автоматически развертывает программное обеспечение в формате MSI на компьютеры домена.

Настройка:

ПКМ на `Software installation` → New → Package...

1. Выберите MSI-пакет из сетевой папки. Важно, чтобы у группы `Domain Computers` были права на чтение из этой папки.
2. Выберите метод развертывания **Assigned**. Программа будет установлена автоматически при следующей перезагрузке компьютера.

Обоснование:

Позволяет централизованно и автоматически устанавливать необходимое ПО на все компьютеры организации без участия пользователя.

Пример команды PowerShell:

```
# This requires the GPO cmdlets from RSAT.
$gpo = Get-GPO -Name "My Software GPO"
$msi = Get-MSIPackageInfo -Path "\\\\server\\share\\app.msi"
#(Advanced usage, typically done via GUI)
```

---

45. ????????? ?????? Windows Update (WSUS)

Configure Windows Update (WSUS)

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Центр обновления Windows
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Update

Описание:

Управляет процессом обновления Windows, позволяя направлять клиенты на внутренний сервер WSUS.

Настройка:

- Включить **Configure Automatic Updates**, выбрав опцию `4 - Auto download and schedule the install`.
- Включить **Specify intranet Microsoft update service location** и указать адрес вашего WSUS-сервера в обоих полях (например, `http://wsus.domain.local:8530`).

Обоснование:

Дает полный контроль над процессом обновлений, экономит интернет-трафик и позволяет тестировать обновления перед их развертыванием на все машины.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows\\WindowsUpdate" -Name "WUServer" -Value "http://wsus.domain.local:8530"
Set-ItemProperty -Path "HKLM:\\Software\\Policies\\Microsoft\\Windows\\WindowsUpdate" -Name "WUStatusServer" -Value "http://wsus.domain.local:8530"
```

---

46. ????????? ??????????? Windows

Configure Windows Defender Firewall

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Брандмауэр Защитника Windows в режиме повышенной безопасности

> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Windows Defender Firewall with Advanced Security

Описание:

Централизованно управляет правилами и состоянием брандмауэра на всех компьютерах.

Настройка:

Здесь можно настроить свойства для каждого профиля (Domain, Private, Public), например, включить брандмауэр и блокировать все входящие по умолчанию.

Для создания правил, ПКМ на `Inbound Rules` → New Rule... Например, можно создать правило, разрешающее ICMP (ping) для диагностики сети.

Обоснование:

Обеспечивает единый стандарт сетевой безопасности в организации, предотвращая отключение брандмауэра пользователями и блокируя нежелательный трафик.

Пример команды PowerShell:

```
New-NetFirewallRule -DisplayName "Allow Ping In" -Direction Inbound -Protocol ICMPv4 -Action Allow
```

---

47. ?????????? ?????? ? ????????? ?????????????

Add group to local administrators

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Настройка -> Параметры панели управления -> Локальные пользователи и группы
>
> **EN:** Computer Configuration -> Preferences -> Control Panel Settings -> Local Users and Groups

Описание:

Централизованно добавляет доменную группу в локальную группу "Администраторы" на всех компьютерах.

Настройка:

ПКМ → New → Local Group.

- **Action:** `Update`.
- **Group name:** `Administrators` (built-in).
- Нажать **Add...** и добавить доменную группу (например, `DOMAIN\IT-Support`).
- Отметить **Delete all member users** и **Delete all member groups**, если нужно, чтобы в локальных администраторах были ТОЛЬКО указанные вами группы.

Обоснование:

Правильный способ предоставления административных прав. Вместо добавления отдельных пользователей на каждой машине, вы управляете членством в одной доменной группе.

Пример команды PowerShell:

```
# This is a preference item, no direct cmdlet.
#To do this locally on one machine:
Add-LocalGroupMember -Group "Administrators" -Member "DOMAIN\\IT-Support"
```

---

48. ????????????? ??????? ? ???????????? ??????

Configure Windows NTP Client

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Система -> Служба времени Windows -> Поставщики времени
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> System -> Windows Time Service -> Time Providers

Описание:

Обеспечивает, чтобы все компьютеры в домене синхронизировали время с контроллера домена.

Настройка:

Включить (Enable) политику `Configure Windows NTP Client`. В поле `NtpServer` указать DNS-имя вашего КД с флагом `,0x9` (например, `dc1.domain.local,0x9`). Установить `Type` в `NTP`.

Обоснование:

Критически важно для корректной работы аутентификации Kerberos, которая чувствительна к расхождению времени между клиентом и сервером.

Пример команды PowerShell:

```
w32tm /config /manualpeerlist:"dc1.domain.local,0x9" /syncfromflags:manual /reliable:yes
/update
```

---

49. ???????? WinRM

Enable Windows Remote Management (WinRM)

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Удаленное управление Windows (WinRM) -> Служба WinRM
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service

Описание:

Разрешает удаленное управление компьютерами с помощью PowerShell.

Настройка:

Включить (Enable) политику `Allow remote server management through WinRM` и указать диапазон IP-адресов для фильтра (например, `192.168.1.0/24` или `*` для всех).

Обоснование:

Основа для современной автоматизации и удаленного администрирования Windows. Позволяет выполнять PowerShell скрипты на множестве машин с одной консоли.

Пример команды PowerShell:

```
# Command to enable WinRM locally. GPO sets this remotely.
Enable-PSRemoting -Force
```

---

50. ????????? ???????? ?????????? PowerShell

Turn on Script Execution

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Административные шаблоны -> Компоненты Windows -> Windows PowerShell
>
> **EN:** Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows PowerShell

Описание:

Устанавливает политику выполнения скриптов PowerShell для всей организации.

Настройка:

Включить (Enable) политику и выбрать одну из опций. Рекомендуется `RemoteSigned` - разрешает выполнение локальных скриптов, а скачанные из интернета должны быть подписаны.

Обоснование:

Базовый механизм безопасности PowerShell, который предотвращает случайный запуск вредоносных скриптов. Централизованная настройка через GPO обеспечивает единый стандарт безопасности.

Пример команды PowerShell:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine
```

---

51. ????????? ?????? ? ????? %windir%\\system32\\drivers\\etc

Restrict access to drivers folder

Путь в редакторе GPO:

> **RU:** Конфигурация компьютера -> Политики -> Конфигурация Windows -> Параметры безопасности -> Файловая система

> **EN:** Computer Configuration -> Policies -> Windows Settings -> Security Settings -> File System

Описание:

Устанавливает права доступа на уровне файловой системы, чтобы запретить пользователям изменять файл hosts.

Настройка:

ПКМ → Add File... → указать путь `%windir%\\system32\\drivers\\etc`. В настройках безопасности удалить права на запись для группы "Пользователи" (Users).

Обоснование:

Защищает от атак, при которых вредоносное ПО изменяет файл `hosts`, чтобы перенаправить пользователя с легитимного сайта (например, банка) на фишинговый.

Пример команды PowerShell:

```
# This is a file system ACL change, no direct cmdlet.
#Example to view ACL for the hosts file:
Get-Acl C:\\Windows\\System32\\drivers\\etc\\hosts | Format-List
```

---

52. ????????????? ?????????

Deploy Printers

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Настройка -> Параметры панели управления -> Принтеры
>
> **EN:** User Configuration -> Preferences -> Control Panel Settings -> Printers

Описание:

Удобный способ назначать пользователям сетевые принтеры.

Настройка:

ПКМ → New → Shared Printer. Выбрать `Action: Update` и указать UNC-путь к принтеру (`\\print-server\Kyocera-Office`). Можно настроить нацеливание на уровне элемента, чтобы принтер назначался только членам определенной группы безопасности.

Обоснование:

Полностью автоматизирует установку принтеров для пользователей, избавляя от необходимости делать это вручную на каждом рабочем месте.

Пример команды PowerShell:

```
# Printer deployment via GPO Preferences не имеет прямого командлета.
#Пример добавления принтера для текущего сеанса:
Add-Printer -ConnectionName "\\\\print-server\\Kyocera-Office"
```

---

53. ????????? ??????-???????

Configure Proxy Settings

Путь в редакторе GPO:

> **RU:** Конфигурация пользователя -> Настройка -> Параметры панели управления -> Параметры обозревателя
>
> **EN:** User Configuration -> Preferences -> Control Panel Settings -> Internet Settings

Описание:

Централизованно настраивает параметры прокси-сервера для пользователей.

Настройка:

ПКМ → New → Internet Explorer 10. На вкладке "Connections" нажать "LAN Settings" и указать адрес и порт прокси-сервера.

Обоснование:

Обеспечивает, чтобы весь интернет-трафик пользователей проходил через корпоративный прокси-сервер для фильтрации контента, учета и безопасности.

Пример команды PowerShell:

```
Set-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet
Settings" -Name "ProxyEnable" -Value 1
Set-ItemProperty -Path "HKCU:\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet
Settings" -Name "ProxyServer" -Value "proxy.domain.local:8080"
```

Revision #1
Created 5 October 2025 21:37:25 by Admin
Updated 5 October 2025 21:41:57 by Admin