

Защита АСУ ТП здесь и сейчас

Рекомендации для встроенных механизмов
защиты компонентов АСУ ТП

Версия

1.0

Дата

04.03.2022

Оглавление

1 Введение.....	3
2 Сетевые сервисы.....	3
3 Настройки учетных записей.....	3
4 Локальные политики безопасности.....	5
5 Аудит безопасности.....	6
6 Обновления.....	7
7 Удаленный доступ.....	7
Наши контакты.....	7
Приложение А. Рекомендации по настройке ОС Windows.....	8

1 Введение

Мы подготовили список рекомендаций для встроенных механизмов защиты компонентов АСУ ТП – рабочих станций, серверов, активного сетевого оборудования, ПЛК. Это рекомендации, которые можно применить на практике, чтобы:

- проверить свою систему обеспечения ИБ на предмет адекватности выполненных настроек и наличия отклонений от безопасного состояния, вызванных изменениями в ходе эксплуатации;
- принять меры защиты «здесь и сейчас», когда нет времени и ресурсов на согласование бюджетов и проектирование системы обеспечения ИБ.

2 Сетевые сервисы

Сетевые сервисы могут являться точками проникновения нарушителей в защищаемые системы путем использования уязвимостей программного кода сервисов или их настроек. Задача защиты сводится к инвентаризации сетевых сервисов, которые могут быть использованы злоумышленниками, и уменьшению поверхности атак:

- Отключение неиспользуемых сетевых служб. Отключение служб веб-сервера, файлового сервера, сервера точного времени и других там, где эти службы не требуются. Отключение сервисов удаленного управления, таких как Web или FTP, на ПЛК.
- Для ОС Windows рекомендуется отключить следующие сервисы:
 - Clipboard.
 - Fax service.
 - Help and support.
 - Messenger.
 - Microsoft POP3 service.
 - NetMeeting remote desktop sharing.
 - Network News Transport Protocol (NNTP).
 - Print server for Macintosh.
 - Simple Mail Transfer Protocol (SMTP).
 - Telephony.
 - Trivial FTP daemon.
 - Wireless configuration.
 - Windows Media Server.

Иные сервисы возможно отключить после оценки влияния на функции защищаемой системы.

- Отключение сетевых сервисов, имеющих уязвимости, либо устранение уязвимостей путем установки обновлений и/или применения безопасных настроек. Например, отключение SNMPv1 на сетевом и инженерном оборудовании.
- Перевод сетевых сервисов на использование безопасных протоколов передачи данных. Замена Telnet на SSH, http на https. Отказ от использования устаревших уязвимых протоколов со слабой защитой данных, либо передающих данные в открытом виде.
- Использование встроенных функций фильтрации сетевых пакетов. Актуально для сетевых узлов под управлением ОС Windows, ОС Linux, активного сетевого оборудования, ПЛК, инженерного оборудования и других. Локальные сетевые экраны должны быть включены, должны разрешать только тот трафик, который нужен для функционирования защищаемой системы. Весь остальной трафик должен попадать под последнее правило – запрета прохождения пакетов.

3 Настройки учетных записей

Используя слабости в настройках учетных записей нарушители также могут получить доступ к защищаемым системам. Задача – усилить парольные политики и предотвратить

возможность получения пользовательских секретов:

- Для привилегированных пользователей и учетных записей служб рекомендуется применение сложных и длинных паролей, а также их частая смена.
- Для пользователей с рядовыми правами также необходима периодическая смена паролей и выполнение требований сложности и уникальности.
- Для снижения вероятности угадывания имен учетных записей рекомендуется изменение учетных записей по умолчанию – Admin или User рекомендуется заменить на нетиповые логины.
- Отключение неиспользуемых учетных записей и учетной записи гостя.
- Отключение обратимого шифрования при хранении секретов.
- Для SCADA и ПЛК (актуально и для других компонентов АСУ ТП) необходимо изменить стандартные и пустые пароли в соответствующих настройках.

Пример парольной политики для ОС семейства Windows приведен на рисунках 1 и 2.

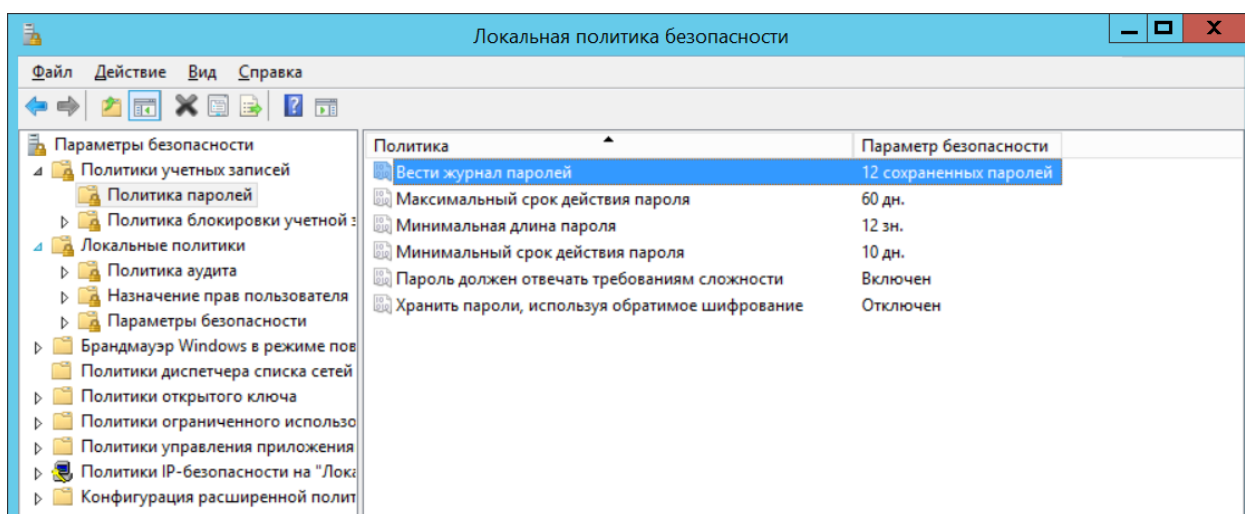


Рисунок 1 – Политика паролей ОС Windows

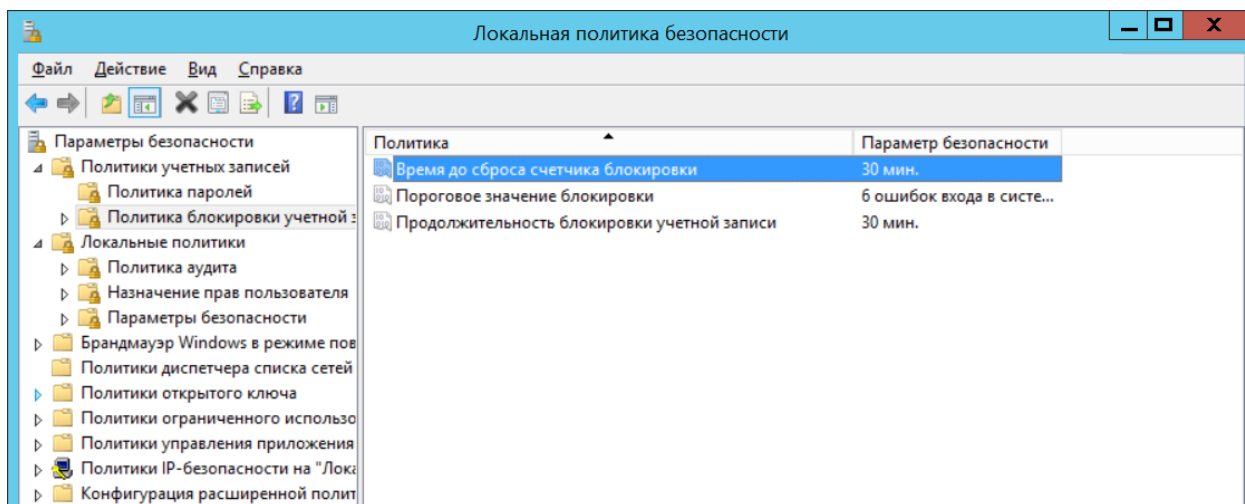


Рисунок 2 – Политика блокировки учетных записей

Относительно настроек блокировки учетных записей следует сопоставить риск блокирования учетной записи и невозможность выполнения производственных задач и возможности по блокировке нарушителя. Зачастую вместо принудительной блокировки учетных записей более эффективно осуществлять мониторинг событий входа в ОС и своевременно реагировать на массовые неуспешные попытки аутентификации.

Настройки парольных политик для ОС Linux различны для различных дистрибутивов

ОС и могут быть найдены в документации на ОС или статьях <https://ostechnix.com/how-to-set-password-policies-in-linux/>

4 Локальные политики безопасности

Настройка локальных политик безопасности позволяет применить встроенные механизмы защиты сетевых узлов и существенно повысить их уровень защищенности. В составе ОС семейства Windows присутствуют шаблоны безопасности, которые определяют безопасные, но жесткие настройки ОС. Однако применяя встроенные шаблоны безопасности без должного анализа и адаптации существует возможность не только значительно повысить уровень защищенности узла, но и повлиять на функционирование его сервисов.

Обобщенные рекомендации по настройке встроенных механизмов ОС Windows приведены в Приложении А.

Существует ряд рекомендаций производителей АСУ ТП, определяющих важные настройки локальных политик безопасности и протестированных с соответствующим ПО АСУ ТП. Эти документы могут быть найдены в сети Интернет или запрошены у производителя АСУ ТП.

Например, Siemens публикует рекомендации в документе «[Recommended security settings for IPCs in industrial environments](#)». Пример автоматизированной проверки на соответствие требованиям этого документа средствами CL DATAPK приведен на рисунке 3.

Информация о рекомендации в документации Siemens «Recommended security settings for IPCs in industrial environments»	Проверяемый параметр	Соответствует ли рекомендациям Siemens
Раздел 4.2 документации: «Обнаружение пользовательской установки и запроса повышения прав с помощью контроля учетных записей пользователей (UAC)». Параметр: Локальная политика безопасности\Локальные политики\Параметры безопасности\Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей (рекомендуемое значение: «Автоматически отклонять запросы на повышение прав»)	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorUser	Не соответствует
Раздел 4.4 документации: «Запрет завершения работы системы без выполнения входа в систему». Параметр: Локальная политика безопасности\Локальные политики\Параметры безопасности\Завершение работы: разрешить завершение работы системы без выполнения входа в систему (рекомендуемое значение: «Отключен»)	MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\ShutdownWithoutLogon	Соответствует

Рисунок 3 – Проверка выполнения требований документа Siemens средствами CL DATAPK

Для примера рассмотрим ПЛК Siemens S7-300. Для обеспечения безопасности программы и данных в ПЛК Siemens S7-300 предусмотрены встроенные механизмы защиты. Необходимо их настроить и осуществлять периодический контроль. Пример контроля параметров безопасности для ПЛК Siemens S7-300 приведен на рисунке 4.

Параметр	Значение
Собрано блоков	111/111
Код заказа	6E57 315-2EH14-0AB0
Версия ОС	37.12.12
Тип модуля	CPU 315-2 PN/DP
Серийный номер	S C-H5D527772016
Наименование ПЛК	S7300/ET200M station_1
Наименование модуля	PLC_1
Состояние ПЛК	S7CpuStatusRun
Количество программных блоков	111
Позиция селектора	RUN-P
Параметры уровня защиты	Write Password
Уровень защиты ЦПУ	Read Only
Переключатель запуска	Unknown / N.A.
Уровень защиты селектора	Can Read/Write

Рисунок 4 – Пример контроля параметров безопасности ПЛК Siemens S7-300

Что касается ОС Linux, то данное семейство ОС также предоставляет встроенные механизмы ИБ. Например, ОС Linux имеет встроенную систему принудительного контроля доступа SELinux, повышающую уровень защищенности и рекомендованную к настройке и включению.

5 Аудит безопасности

Встроенные средства компонентов АСУ ТП зачастую позволяют регистрировать события безопасности, такие как вход и выход, попытки ввода паролей и другие события, которые могут позволить выявить инцидент ИБ и своевременно его предотвратить. Рекомендуется включить аудит событий безопасности на всех компонентах АСУ ТП – рабочих местах и серверах, ОС и специальном ПО, сетевом оборудовании и ПЛК при наличии технической возможности.

Настройки аудита ОС Windows и журналов приведены в Приложении А.

Для примера настройки аудита SCADA Siemens WinCC 7.0 включаются следующим образом:

1. Необходимо открыть редактор «Alarm Logging» (WinCC Explorer -> Project Name -> Alarm Logging)
2. Далее вызвать диалоговое окно «WinCC System Messages» (Tools -> WinCC System Messages)

3. В поле «A User text block is required for displaying system message texts. Please select a user text block» выбрать «WinCC message text». В поле «Create system messages» отметить «Create only new system messages», нажать кнопку «Create».
4. После завершения установки нажать кнопку «Close».

6 Обновления

С целью устранения уязвимостей и ошибок функционирования, а также получения баз решающих правил в случае со средствами защиты информации, необходимо применять обновления для всех компонентов АСУ ТП и системы защиты.

С учетом высокой критичности технологических процессов наша рекомендация – установка обновлений ПО для компонентов АСУ ТП и баз решающих правил средств защиты информации должна осуществляться только после их тестирования и принятия решения об отсутствии негативного влияния на защищаемую систему.

7 Удаленный доступ

Рекомендуется запретить удаленный доступ к компонентам АСУ ТП из сети Интернет и других сетей, внешних по отношению к защищаемым АСУ ТП (например, корпоративной). При необходимости реализации удаленного подключения к АСУ ТП рекомендуется использование опосредованного доступа через терминальные серверы / VDI, размещенные в демилитаризованной зоне, с применением средств двухфакторной аутентификации и специализированных комплексов контроля действий привилегированных пользователей.

Наши контакты

Если у вас есть вопросы по защите промышленных систем автоматизации или вопросы по решениям и услугам компании СайберЛимфа, вы всегда можете связаться с нами по электронной почте info@cyberlympha.com или через форму обратной связи на сайте компании <https://cyberlympha.ru>

Приложение А. Рекомендации по настройке ОС Windows

Параметр	Значение
Назначение прав пользователя	
Архивация файлов и каталогов	BUILTIN\Администраторы
Блокировка страниц в памяти	
Восстановление файлов и каталогов	BUILTIN\Администраторы
Выполнение задач по обслуживанию томов	BUILTIN\Администраторы
Добавление рабочих станций к домену	BUILTIN\Администраторы
Доступ к компьютеру из сети	NT AUTHORITY\Прошедшие проверку, BUILTIN\Администраторы
Завершение работы системы	BUILTIN\Администраторы
Загрузка и выгрузка драйверов устройств	BUILTIN\Администраторы
Замена маркера уровня процесса	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Запретить вход в систему через службу терминалов	NT AUTHORITY\Локальная учетная запись, BUILTIN\Гости
Запретить локальный вход	BUILTIN\Гости
Изменение метки объекта	
Изменение параметров среды изготовителя	BUILTIN\Администраторы
Изменение системного времени	BUILTIN\Администраторы, NT AUTHORITY\LOCAL SERVICE
Изменение часового пояса	BUILTIN\Администраторы, NT AUTHORITY\LOCAL SERVICE
Имитация клиента после проверки подлинности	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\СЛУЖБА, BUILTIN\Администраторы
Локальный вход в систему	BUILTIN\Администраторы
Настройка квот памяти для процесса	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, BUILTIN\Администраторы
Отказ в доступе к компьютеру из сети	NT AUTHORITY\Локальная учетная запись, BUILTIN\Гости
Отказ во входе в качестве пакетного задания	BUILTIN\Гости
Отказать во входе в качестве службы	BUILTIN\Гости
Отладка программ	BUILTIN\Администраторы
Принудительное удаленное завершение работы	BUILTIN\Администраторы
Профилирование одного процесса	BUILTIN\Администраторы
Работа в режиме операционной системы	
Разрешать вход в систему через службу терминалов	BUILTIN\Администраторы
Разрешение доверия к учетным записям компьютеров и пользователей при делегировании	
Смена владельцев файлов и других объектов	BUILTIN\Администраторы
Создание аудитов безопасности	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE
Создание глобальных объектов	NT AUTHORITY\NETWORK SERVICE, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\СЛУЖБА, BUILTIN\Администраторы
Создание маркерного объекта	
Создание постоянных общих объектов	
Создание символических ссылок	BUILTIN\Администраторы
Создание файла подкачки	BUILTIN\Администраторы
Увеличение приоритета выполнения	BUILTIN\Администраторы
Управление аудитом и журналом безопасности	BUILTIN\Администраторы

Параметр	Значение
Параметры безопасности	
Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности	Отключено
Сетевой доступ: запретить анонимный доступ к именованным каналам и общим ресурсам	Включено
Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей	Обычная - локальные пользователи удостоверяются как они сами
Сетевой доступ: не разрешать перечисление учетных записей SAM анонимными пользователями	Включено
Сетевой доступ: не разрешать перечисление учетных записей SAM и общих ресурсов анонимными пользователями	Включено
Сетевой доступ: разрешать применение разрешений «Для всех» к анонимным пользователям	Отключено
Сетевой доступ: удаленно доступные пути и вложенные пути реестра	System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\UserConfig, System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration, Software\Microsoft\Windows NT\CurrentVersion\Perflib, System\CurrentControlSet\Services\SysmonLog
Завершение работы: очистка файла подкачки виртуальной памяти	Отключено
Завершение работы: разрешить завершение работы системы без выполнения входа в систему	Отключено
Интерактивный вход в систему: поведение при извлечении смарт-карты	Блокировка рабочей станции
Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее	14 дн.
Интерактивный вход в систему: не отображать последнее имя пользователя	Включено
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Отключено
Клиент сети Microsoft: использовать цифровую подпись (всегда)	Включено
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включено
Клиент сети Microsoft: отправлять незашифрованный пароль сторонним SMB-серверам	Отключено
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Включено

Параметр	Значение
Контроль учетных записей: обнаружение установки приложений и запрос на повышение прав	Включено
Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав	Включено
Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором	Запрос согласия на безопасном рабочем столе
Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей	Автоматически отклонять запросы на повышение прав
Контроль учетных записей: повышать права для UIAccess-приложений только при установке в безопасных местах	Включено
Контроль учетных записей: при сбоях записи в файл или реестр виртуализация в место размещения пользователя	Включено
Контроль учетных записей: разрешить UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол	Отключено
Параметр	Значение
Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Включено
Сетевая безопасность: минимальная сеансовая безопасность для клиентов на базе NTLM SSP (включая безопасный RPC)	Включено; Требовать сеансовую безопасность NTLMv2: Включено; Требовать 128-битное шифрование: Включено
Сетевая безопасность: минимальная сеансовая безопасность для серверов на базе NTLM SSP (включая безопасный RPC)	Включено; Требовать сеансовую безопасность NTLMv2: Включено; Требовать 128-битное шифрование: Включено
Сетевая безопасность: не хранить хэш-значения LAN Manager при следующей смене пароля	Включено
Сетевая безопасность: требование цифровой подписи для LDAP-клиента	Согласование цифровой подписи
Сетевая безопасность: уровень проверки подлинности LAN Manager	Отправлять только NTLMv2-ответ. Отказывать LM и NTLM
Системные объекты: усилить разрешения по умолчанию для внутренних системных объектов (например, символических ссылок)	Включено
Системные объекты: учитывать регистр для подсистем, отличных от Windows	Включено
Параметры системы: использовать правила сертификатов для исполняемых файлов Windows для политик ограниченного использования программ	Включено
Устройства: запретить пользователям установку драйверов принтера	Включено
Устройства: разрешить форматирование и извлечение съемных носителей	Администраторы
Учетные записи: разрешить использование пустых паролей только при консольном входе	Включено

Параметр	Значение
Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Vista или следующие версии)	Включено
Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена)	4 входов в систему
Параметр	Значение
Интерактивный вход в систему: пороговое число неудачных попыток входа	10 до блокировки учетной записи компьютера
Интерактивный вход в систему: предел простоя компьютера	900 сек.
Консоль восстановления: разрешить автоматический вход администратора	Отключено
Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам	Отключено
Сервер сети Microsoft: время бездействия до приостановки сеанса	15 мин.
Сервер сети Microsoft: использовать цифровую подпись (всегда)	Включено
Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	Включено
Сервер сети Microsoft: отключать клиентов по истечении разрешенных часов входа	Включено
Сетевая безопасность: разрешить LocalSystem использовать нулевые сеансы	Отключено
Сетевая безопасность: разрешить учетной записи локальной системы использовать удостоверение компьютера для NTLM	Включено
Член домена: всегда требуется цифровая подпись или шифрование потока данных безопасного канала	Включено
Член домена: отключить изменение пароля учетных записей компьютера	Отключено
Член домена: требовать стойкий сеансовый ключ (Windows 2000 или выше)	Включено
Член домена: цифровая подпись данных безопасного канала, когда это возможно	Включено
Член домена: шифрование данных безопасного канала, когда это возможно	Включено
Политики аудита	
Вход учетной записи: Аудит проверки учетных данных	Успех, отказ
Управление учетными записями: Аудит управления учетными записями компьютеров	Успех
Управление учетными записями: Аудит других событий управления учетными записями	Успех, отказ
Управление учетными записями: Аудит управления группами безопасности	Успех, отказ
Управление учетными записями: Аудит управления учетными записями пользователей	Успех, отказ
Подробное отслеживание: Аудит создания процессов	Успех
Подробное отслеживание: Аудит завершения процессов	Успех
Вход/выход: Аудит блокировки учетных записей	Успех

Параметр	Значение
Вход/выход: Аудит выхода из системы	Успех
Вход/выход: Аудит входа в систему	Успех, отказ
Вход/выход: Аудит специального входа	Успех
Доступ к объектам: Аудит файловой системы	Успех, отказ
Изменение политики: Аудит изменения политики аудита	Успех, отказ
Изменение политики: Аудит изменения политики проверки подлинности	Успех
Использование прав: Аудит использования прав, затрагивающих конфиденциальные данные	Успех, отказ
Система: Аудит драйвера IPsec	Успех, отказ
Система: Аудит других системных событий	Успех, отказ
Система: Аудит изменения состояния безопасности	Успех, отказ
Система: Аудит расширения системы безопасности	Успех, отказ
Система: Аудит целостности системы	Успех, отказ
Журнал событий	
Maximum application log size	16384 kilobytes
Maximum security log size	81920 kilobytes
Maximum system log size	16384 kilobytes
Prevent local guests group from accessing application log	Enabled
Prevent local guests group from accessing security log	Enabled
Prevent local guests group from accessing system log	Enabled
Retention method for application log	As needed
Retention method for security log	As needed
Retention method for system log	As needed