КИБЕРПРОТЕКТ

Кибер Файлы 8.6.2

РУКОВОДСТВО АДМИНИСТРАТОРА

Редакция: 29.04.2022

Оглавление

1 Общие сведения о продукте Кибер Файлы

Продукт Кибер Файлы должен представлять собой решение для безопасного доступа, синхронизации и совместного использования файлов организации. Решение должно позволять IT-отделу организации контролировать безопасность передаваемого контента и соблюдения нормативных требований.

Необходимо реализовать возможность использовать Кибер Файлы на разных устройствах - настольных компьютерах, ноутбуках, планшетах или смартфонах. Пользователям нужно дать возможность обмениваться файлами не только внутри компании, но и с внешними доверенными лицами, например, клиентами, партнерами и поставщиками.

Функциональные возможности программы должны быть следующие: доступ и синхронизация данных и совместное использование.

Программа Кибер Файлы должна позволять корпоративным ИТ-отделам осуществлять контроль над доступом к файлам и определять, соответствуют ли действия по обмену файлами нормативным требованиям и требованиям безопасности организации. Кроме того программа Кибер Файлы должна обеспечивать уровень видимости и мониторинга, недоступный для потребительских решений.

Необходимо реализовать в программе уровень видимости и мониторинга, недоступный для потребительских решений.

2 Требования к архитектуре

Требуется разработать программу Кибер Файлы в следующих вариантах:

- Веб- сервер. Должна позволять администраторам устанавливать программу на сервер, администрировать программу и давать доступ пользователям.
- Веб-клиент. Должен позволять пользователям совместно использовать файлы и папки через веб-браузер.
- Клиент для ПК, мобильный шлюз и файловый репозиторий. Должен позволять пользователям совместно использовать файлы и папки через приложение для ПК.

2.1 Требования к конфигурации

Для установки программы на сервер требуется создать утилиту настройки, которая позволит пользователям настроить доступ к серверу Кибер Файлы, репозиторию файлов и веб-серверу.

Должна быть возможность изменять параметры утилиты настройки в любое время. Утилита должна автоматически изменять необходимые файлы конфигурации и перезапускать соответствующие службы.

2.1.1 Веб-сервер

Веб-сервер должен представлять собой веб-интерфейс пользователя для клиентов программы, а также консоль администрирования для мобильного доступа к программе и компонент синхронизации данных.

В утилите настройки должны быть доступны следующие параметры веб-сервера:

- **Адрес** – IP-адрес веб-интерфейса.
- **Порт** – порт веб-интерфейса.
- **Сертификат** – путь к сертификату для веб-интерфейса. Должна быть возможность выбрать сертификат из хранилища сертификатов Microsoft Windows.
- **Сертификат цепочки** – путь к промежуточному сертификату для веб-интерфейса. Должна быть возможность выбрать сертификат из хранилища сертификатов Microsoft Windows. Этот сертификат необходим только в случае, если центр сертификации также выдал промежуточный сертификат.

2.1.2 Мобильный шлюз

Мобильный шлюз должен предоставлять мобильным клиентам возможность доступа к файлам и к общим ресурсам.

В утилите настройки должны быть доступны следующие параметры мобильного шлюза:

- **Адрес** – IP-адрес сервера шлюза.
- **Порт** – порт подключения к серверу шлюза.

- **Сертификат** – путь к сертификату сервера для вашего шлюзового сервера. Должна быть возможность выбрать сертификат из хранилища сертификатов Microsoft Windows.

2.1.3 Файловый репозиторий

Файловый репозиторий должен представлять собой хранилище, которое Кибер Файлы используют для синхронизации данных. Путь к хранилищу файлов должен указывать местоположение на диске, которое будет использоваться в качестве хранилища.

В утилите настройки должны быть доступны следующие параметры файлового репозитория:

- **Адрес** – IP-адрес файлового репозитория.
- **Порт** – порт подключения к файловому репозиторию.
- **Путь к файловому репозиторию** – путь к хранилищу файлов в UNC-формате. При изменении пути к хранилищу файлов НЕОБХОДИМО вручную скопировать все файлы из исходного хранилища в новое место.
- **Учетная запись службы** – если хранилище файлов репозитория расположено на удаленном сетевом ресурсе, то необходимо настроить учетную запись службы, у которой есть разрешения на работу с этим сетевым общим ресурсом. У этой учетной записи также должны быть права на чтение и запись в папке репозитория, чтобы иметь возможность записи в файл журнала.

2.2 Требования к кластеризации

Программа Кибер Файлы должна позволять настраивать параметры высокой доступности без использования стороннего программного обеспечения для кластеризации. Необходимо реализовать функцию кластеризации в программе, и также поддержать отказоустойчивую кластеризацию Microsoft.

2.3 Требования к балансировке нагрузки

Программа Кибер Файлы должна поддерживать балансировку нагрузки. Рекомендуемая конфигурация - разделить все части Кибер Файлы Сервер на отдельных машинах за балансировщиками нагрузки. Файловый репозиторий и хранилище файлов могут размещаться на одном компьютере.

Перед переносом рабочего сервера слудует рекомендовать пользователям выполнить шаги настройки в тестовой среде. Тестовое развертывание должно иметь ту же архитектуру, что и рабочие серверы, а также пару тестовых пользовательских компьютеров и мобильных клиентов, чтобы обеспечить совместимость в среде пользователя.

3 Аппаратные и программные требования

Для установки программы Кибер Файлы на сервер требуется учетная заись администратора.

Для работы программы должны выполняться следующие требования.

3.1 Требования к операционным системам

3.1.1 Рекомендуемая совместимость с операционными системами:

- Windows Server 2016 Standard и центр обработки данных;
- Windows Server 2012 R2 Standard или Datacenter.

3.1.2 Также должны поддерживаться операционные системы:

- Windows Server 2019 Standard и центр обработки данных;
- Windows Server 2016 Standard и центр обработки данных;
- Windows Server 2012 R2 Standard или Datacenter;
- Windows Server 2012 Standard или Datacenter.

3.2 Требования к оборудованию

3.2.1 Примеры развертываний

Эти цифры развертывания предполагают, что все компоненты Кибер Файлов работают на одной виртуальной машине или физическом сервере.

Небольшие развертывания

- До 25 пользователей.
- Процессор: Intel i7 Xeon class с 4 ядрами или аналог AMD.
- Оперативная память: 16 ГБ.
- Место на диске: 100 ГБ.

Средние развертывания

- До 500 пользователей.
- Процессор: Intel i7 Xeon класса с 8 ядрами или аналог AMD.
- Оперативная память: 40 ГБ.
- Дисковое пространство: 2 ТБ RAID.

Крупные развертывания

- До 2500 пользователей.
- Процессор: Intel i7 Xeon class с 16 ядрами или аналог AMD.
- Оперативная память: 64 ГБ.
- Дисковое пространство: 10 ТБ RAID.

Примечание
Для развертываний с числом пользователей более 2500 рекомендуется кластерная конфигурация сервера.

3.3 Сетевые требования

- Один статический IP-адрес. Для определенных конфигураций может потребоваться два IP-адреса.
- Необязательно, но рекомендуется: имена DNS, соответствующие указанным выше IP-адресам.
- Сетевой доступ к контроллеру домена, если планируется использовать Active Directory (LDAP).
- Сетевой доступ к SMTP-серверу для уведомлений и приглашений по электронной почте.
- Адрес **127.0.0.1** должен использоваться мобильным приложением для внутренних целей и не должен участвовать в туннелях какого-либо вида: VPN, MobileIron, BlackBerryDynamics и т. д.
- Все машины должны быть привязаны к Windows Active Directory.

HTTPS-трафик должен обрабатываться сервером шлюза и веб-сервером. Сервер шлюза используется мобильными клиентами для доступа к файлам и общим ресурсам источников данных. Веб-сервер предоставляет веб-интерфейс для синхронизации данных а также является административной консолью для мобильного доступа и синхронизации данных.

Для большинства развертываний рекомендуется назначить обоим серверам один IP-адрес, но с разными портами и отдельными DNS-записями. Конфигурация с одним IP-адресом подойдет для большинства установок. Сервер можно настроить на использование отдельных IP-адресов для каждого компонента, если этого требует конкретная модель развертывания или установки.

Если нужно предоставлять доступ мобильным устройствам за пределами файрвола, должно быть реализовано несколько вариантов для пользователей.

- **Доступ к порту 443:** Программа Кибер Файлы должна использовать HTTPS для зашифрованного транспорта. Если пользователь откроет порт 443 для доступа к веб-серверу, авторизованные клиенты должны иметь возможность подключаться как внутри, так и за пределами файрвола.
- **VPN:** Программа Кибер Файлы должна поддерживать доступ через VPN-соединение. Должен поддерживаться как встроенный клиент iOS VPN, так и сторонние клиенты VPN. Профили управления iOS можно дополнительно применить к устройствам, использующим системы управления мобильными устройствами (MDM) или программу настройки Apple iPhone, чтобы

настроить функцию iOS VPN-по-запросу на основе сертификатов, обеспечивая беспрепятственный доступ к Кибер Файлам.

- **Обратный прокси-сервер:** Программа Кибер Файлы должна поддерживать сквозную проверку подлинности обратного прокси, проверку подлинности по имени пользователя и паролю, ограниченное делегирование проверки подлинности Kerberos и проверку подлинности сертификата.

3.4 Требования к клиенту для ПК

3.4.1 Системные требования

Поддерживаемые операционные системы:

- Windows 7, Windows 8 и 8.1, Windows 10;
- macOS X от 10.13 до 10.15 с Mac, совместимым с 64-разрядным программным обеспечением;
- macOS 11 Big Sur на чипах Intel x86 и Apple ARM.

Поддерживаемые веб-браузеры:

- Mozilla Firefox 60 и более поздние версии;
- Internet Explorer 10 и более поздние версии;
- Microsoft Edge 42 или более поздняя версия;
- Google Chrome 64 и более поздние версии;
- Safari 12 и более поздние версии;
- Opera 72 и более поздние версии.

3.4.2 Дополнительные требования

- Исполняемый файл установщика Клиента для ПК и соответствующие права для его запуска.
- Адрес сервера, который будет использоваться (предоставляется администратором или по электронной почте).
- Учетные данные для сервера (полученные из Active Directory, предоставленные администратором или по электронной почте).

4 Требования к мастеру настройки программы

Мастер настройки должен помочь администратору выполнить ряд шагов, чтобы обеспечить работу базовых функций сервера.

Настройка программы должна производиться в веб-интерфейсе под учетной записью администратора программы.

4.0.1 Должна быть доступна настройка следующих параметров:

- Лицензирование с возможностью добавить лицензионные ключи.
- Общие настройки: имя сервера, DNS-имя или IP-адрес, с помощью которых пользователь может получить доступ к веб-сайту (начинается с http:// или https://), язык по умолчанию.
- SMTP: DNS-имя или IP-адрес SMTP-сервера, порт подключения, настройка SMTP-аутентификации.
- LDAP: DNS-имя или IP-адрес LDAP-сервера, порт подключения, настройка безопасного соединения.

5 Требования по управлению пользователями и устройствами

5.1 Требования по управлению устройствами

Как только пользователи подключаются к веб-серверу Кибер Файлов, их устройства должны отобразить в списке в разделе **Устройства**.

Должна быть доступна следующая информация:.

- **Имя пользователя** – отображаемое имя Active Directory (AD) для пользователя LDAP или имя, выбранное эпизодическим пользователем.
- **Имя устройства** – заданное пользователем имя устройства.
- **Модель** – официальное название мобильного устройства пользователя.
- **ОС** – тип и версия операционной системы.
- **Версия** - Версия приложения или клиента для ПК.
- **Статус** - должны быть доступны следующие статусы:
  - Управляется;
  - Управляется, ожидание удаленной очистки данных;
  - Не управляется, выполнена удаленная очистка данных;
  - Не управляется, ожидание удаленной очистки данных;
  - Не управляется пользователем;
  - Данные очищены после неправильного ввода пароля.
- **Последний контакт** - Дата и время последнего соединения между сервером управления и приложением / клиентом для ПК.
- **Политика** – имя и ссылка на политику управления, примененную к пользователю.
- **Действия**
  - **Дополнительная информация** – содержит дополнительные сведения об устройстве и редактируемое поле **Примечания**.
  - **Сброс пароля приложения** (только для мобильных устройств) - сбрасывает пароль блокировки приложения на выбранном устройстве. Для этого необходимо сформировать код подтверждения, используя код сброса пароля, отображаемый на экране устройства пользователя.
  - **Удаленная очистка** (только для мобильных устройств) - если выбрано, все файлы вприложении и его собственные настройки удаляются после подключения устройства к серверу управления. Другие приложения и данные ОС не затрагиваются.
  - **Удалить из списка** - Удаляет клиент для ПК из списка устройств.

5.1.1 Экспорт сведений об устройствах

Необходимо реализовать возможность экспортировать сведения об устройствах в файл TXT, CSV или XML.

Экспортируемые данные:

1. Имя пользователя.
2. Имя используемого мобильного устройства или компьютера.
3. Модель мобильного устройства.
4. Тип и версия ОС на устройстве.
5. Версия приложения или клиента для ПК.
6. Статус мобильного устройства или клиента для ПК.
7. Дата и время регистрация на веб-сервере Кибер Файлы.
8. Дата и время последнего контакта между приложением или клиентом для ПК и веб-сервером Кибер Файлы.
9. Имя примененной политики пользователей.
10. Примечания.

5.1.2 Удаленный сброс пароля приложения

Приложение Кибер Файлы может быть защищено паролем блокировки, который необходимо ввести при запуске приложения. Если пользователь забудет этот пароль, он не сможет получить доступ Кибер Файлы. Пароль приложения не связан с паролем учетной записи пользователя в Active Directory.

Необходимо реализовать возможность удаленного сброса пароля на случай если пароль блокировки приложения утерян.

5.1.3 Удаленная очистка данных приложения

Необходимо реализовать возможность удаленно стереть мобильное приложение Кибер Файлы, удалив все файлы, которые хранятся локально или кэшируются в приложении Кибер Файлы.

5.2 Требования по управлению пользователями

Необходимо реализовать возможность управлять всеми пользователями программы Кибер Файлы.

Должна быть возможность пригласить новых пользователей, изменить или удалить текущих пользователей. При изменении пользователя должна быть возможность предоставить ему права администратора, изменить адрес электронной почты, пароль либо отключить (включить) его учетную запись.

5.2.1 Типы пользователей

Необходимо реализовать три типа пользователей программы.

Внешние (эпизодические) учетные записи пользователей

Эти учетные записи необходимо создавать вручную через приглашения по электронной почте, рассылаемые администратором, либо приглашения других пользователей на содержимое общего доступа (файл или папка).

Должно быть два подтипа внешней учетной записи: **Бесплатный**а также **Лицензированный**.

По умолчанию каждая внешняя учетная запись, вновь создаваемая, является бесплатной. Только администратор может преобразовать бесплатную внешнюю учетную запись в лицензированную внешнюю учетную запись.

Пользователи с лицензированной учетной записью могут создавать, загружать, редактировать и удалять файлы и папки в собственном пространстве синхронизации данных. Они также могут передавать свой контент другим пользователям.

Пользователи с бесплатной учетной записью не имеют пространства синхронизации данных. Если им дать соответствующие права, бесплатные пользователи могут создавать новые файлы, загружать их из других источников, а также редактировать и удалять файлы только в папках, которые им предоставлены. Если они имеют права только для чтения, то они не могут создавать, загружать, изменять и удалять файлы, а могут только просматривать и загружать файлы в папках, которые им предоставлены.

Пользователи с бесплатными учетными записями не могут приглашать новых пользователей в общий ресурс, даже если им были предоставлены такие права во время создания учетной записи.

Если файл предоставлен пользователю с бесплатной учетной записью, то он сможет только просмотреть или загрузить его.

Пользователи бесплатной учетной записи не могут использовать Клиент для ПК или мобильные приложения Кибер Файлы.

Внутренние (LDAP) учетные записи пользователей

Такие учетные записи работают на основе интеграции с Active Directory (AD). Они создаются либо вручную - как Внешние, либо администратором.

Внутренние учетные записи автоматически лицензируются в момент создания.

Пользователи с внутренней учетной записью могут создавать, загружать, редактировать и удалять файлы и папки в собственном пространстве синхронизации данных. Они также могут передавать свой контент другим пользователям.

Они могут использовать Клиент для ПК и мобильные приложения Кибер Файлы.

Учетные записи пользователей без доступа

Это административные учетные записи без доступа к синхронизации и общему доступу. По умолчанию они не лицензируются. Пользователи с этими учетными записями не могут использовать Клиент для ПК и мобильные приложения Кибер Файлы.

Экспорт данных о пользователях

Должна быть возможность экспортировать данные обо всех зарегистрированных пользователях в файл в формате TXT, CSV или XML.

Экспортированные данные:

1. Имя пользователя.
2. Имя входа пользователя (для пользователей LDAP).
3. Универсальное имя участника (для пользователей LDAP).
4. Домен LDAP (для пользователей LDAP).
5. Адрес электронной почты.
6. Имя политики.
7. Статус.
8. Права администратора.
9. Статус лицензирования пользователя.
10. Статус отключения пользователя.
11. Аутентификация LDAP.
12. Количество папок, которые принадлежат пользователю.
13. Количество файлов, которые принадлежат пользователю.
14. Объем контента пользователя (в байтах).
15. Размер квоты пользователя (в байтах).
16. Дата и время последнего входа.

6 Требования по администрированию сервера

6.1 Администрирование сервера

Если вы являетесь администратором и входите в веб-интерфейс, вы можете переключаться между режимами **Администратор** и **Пользователь**.

- Чтобы войти в режиме **Администратор**, Нажмите на значок пользователя и Нажмите кнопку **Консоль администрирования**.
- Чтобы войти в режиме **Пользователь**, Нажмите кнопку Выйти из режима администратора в правом верхнем углу.

Примечание
Администраторы имеют доступ к документации API. Вы можете найти ссылку в нижнем колонтитуле веб-интерфейса, когда вы находитесь в режиме администрирования.

6.2 Администраторы и права доступа

Необходимо реализовать следующие права администратора.

- **Полные права администратора**.
- **Может управлять пользователями**. Включает в себя приглашение новых пользователей, инициализацию группы LDAP, отправку приглашения на регистрацию и управление подключенными мобильными устройствами.
- **Может управлять мобильными источниками данных**. Это права для добавления новых серверов шлюза и источников данных, управления назначенными источниками, серверами шлюза, доступными на клиентах, и источниками данных предыдущих версий.
- **Может управлять мобильными политиками**. Это права для управления политиками пользователей и групп, разрешенными приложениями и стандартными ограничениями доступа.
- **Может просматривать журнал аудита**.