ЧФ «Энигма-Софт»

61072, Украина, г. Харьков, ул. 23 Августа 38, к. 23.
http://enigmasoft.com.ua, office@enigmasoft.com.ua
+380-577-177-977, +380-577- 590-723,+380-577-590-724
+380-50-30-15-155, +380-97-96-14-231, +380-93-30-15-155

Комплекс «Стиль»

Сервер и клиент корпоративного обмена файлами ESFS

Руководство по эксплуатации

Харьков

Оглавление

1. Назначение сервера и клиента ESFS

Сервер и клиент **ESFS** for **Windows**, далее комплекс, предназначен для организации файлового обмена в корпоративных сетях и информационных сетях общего пользования. Прием и передача файлов осуществляется по инициативе удаленных клиентских мест:

1. *Встроенные компоненты ESFS-Client*

   - **«Стиль» - Клиент-Банк** транспорт файлов документов между банком и клиентом;
   - **«Стиль» - Учет товаров и материалов** транспорт репликаций распределенной БД.

2. *Портированная компонента ESFS-Client*

   - Транспорт файлов в системах Клиент-банк третьих фирм между банком и клиентом;
   - Транспорт файлов в системах документооборота корпоративных клиентов;
   - Транспорт файлов в системах резервного копирования корпоративных сетей.

2. Сервер ESFS

2.1. Режимы работы

Установленный* сервер запускается менеджером служб при старте Windows и автоматически начинает обслуживать клиентские подключения в режиме сервера файлового обмена. Управление списком пользователей и режимами работы программы выполняется запуском исполняемого модуля сервера **Esfssvc.exe** с параметрами.

*Для установки сервера используется параметр командной строки **Esfssvc.exe -i** (Раздел 2.5. Параметры командной строки).

2.2. Файлы и пути

Сервер реализован в виде следующих файлов расположенных в одном каталоге:

- **Esfssvc.exe** - Исполняемый модуль сервера;
- **Server.ini** - Файл настроек сервера;
- **Security** - База участников файлового обмена. База содержит имена клиентов и хеш-функции их паролей.

Папка содержащая почтовые ящики клиентов, через которые осуществляется обмен файлами с каждым клиентом, находится:

1. При одноуровневой организации - в каталоге, заданном параметром **root dir** (Раздел 2.4. Файл настроек). Имя почтового ящика клиента совпадает с именем клиента. Структура каталогов файлового обмена с клиентом на стороне сервера при одноуровневой организации каталогов приведена ниже:

./root dir

имя_клиента 1 — Почтовый ящик клиента 1

IN - Каталог с файлами, принятыми от клиента

$ - временное хранилище для принимаемых файлов

OUT - каталог с файлами, передаваемыми клиенту

$ - временное хранилище для передаваемых файлов

LOG - Каталог с файлами протоколов обмена с клиентом 1

имя_клиента 2 - Почтовый ящик клиента 2 ... (и т. д.)

2. При двухуровневой организации — подкаталоги групп клиентов, расположены в каталоге, заданном параметром **root dir** (Раздел 2.4. Файл настроек). Все клиенты должны иметь имена, снабженные префиксами фиксированной длины, определяющими принадлежность клиента к той или иной группе. Длина префикса определяется параметром **Division Chars** (Раздел 2.4. Файл настроек). Имя подкаталога группы клиентов совпадает с префиксом в имени клиента. Имя почтового ящика клиента в подкаталоге группы совпадает с остатком имени клиента. Структура почтовых ящиков клиентов на стороне сервера при двухуровневой организации каталогов приведена ниже:

./root dir

имя_группы 1

имя_клиента 1 \ - Почтовый ящик клиента 1 первой группы

**IN ** - Каталог с файлами, принятыми от клиента

**$ ** - временное хранилище для принимаемых файлов
OUT - каталог с файлами, передаваемыми клиенту
$ \ - временное хранилище для передаваемых файлов
LOG \- Каталог с файлами протоколов обмена с клиентом 1
имя_клиента 2 \- Почтовый ящик клиента 2 первой группы
(. . .)
**имя_группы 2 **
имя_клиента 1 \- Почтовый ящик клиента 1 второй группы
**IN ** - Каталог с файлами, принятыми от клиента
$ \ - временное хранилище для принимаемых файлов
OUT \- каталог с файлами, передаваемыми клиенту
$ \ - временное хранилище для передаваемых файлов
LOG \- Каталог с файлами протоколов обмена с клиентом 1

имя_клиента 2\ - Почтовый ящик клиента 2 второй группы
(. . .)
имя_клиента 3\ - Почтовый ящик клиента 3 второй группы
(. . .)

Полное имя клиента выглядит как <**имя_группы**><**имя_клиента**>, где имя_группы имеет фиксированную длину, заданную в конфигурации.

Пример: Почтовый ящик клиента **UJBTestCli** при заданной длине группы равной 3 будет иметь путь **root\UJB\TestCli**

2.3. Управление

Рабочие параметры **ESFS-Server for Windows** считывает из файла настроек (Раздел 2.4. Файл настроек). Для выполнения дополнительных действий используются параметры командной строки (Раздел 2.5. Параметры командной строки).

2.4. Файл настроек

Файл настроек сервера **server.ini** содержит следующие секции и параметры:

[Registration]

Регистрационный ключ
Key = строка

*Срок действия регистрационного ключ*а
Date = dd/mm/yyyy

[Server]

Путь и наименование папки с почтовыми ящиками клиентов
Root dir = путь
Описание: Относительный путь указывается от папки запуска сервера **Esfssvc.exe.** При запуске сервера с ключом: **Esfssvc.exe -c**<путь>, папка будет создана, а путь к ней записан в файл конфигурации.
Умолчание: **.\root**

Адрес прослушивания входящих подключений
Host = IP-адрес
Описание: Используется, если компьютер находится в нескольких сетях и/или имеет несколько адресов, а необходимо слушать только один.
Умолчание: нет

Порт прослушивания входящих подключений.
Port = номер порта
Описание: На каком порту слушать входящие подключения.
Умолчание: 7000

Время ожидания при работе с сокетами
sock timeout = число секунд
Описание: Если по истечении заданного времени от клиента не поступило никаких команд или данных, соединение закрывается.
Умолчание: 30

Двухуровневая организация почтовых ящиков клиентов
Division Chars = число
Описание: Количество лидирующих символов в имени клиента, определяющих имя папки 1-го уровня. В этой папке находятся почтовый ящик клиента (2-й уровень) с его остаточным именем.
Умолчание: 0 (Одноуровневая организация)

Способ авторизации клиента
Authentication = Пусто/LDAP
Описание: По умолчанию авторизация клиента производится по базе клиентов. Для авторизации через LDAP данный параметр должен содержать "LDAP". Остальные параметры задаются в секции **[LDAP]**.
Умолчание: Пусто

Имя файла БД клиентов
Users File = имя файла БД клиентов
Описание: Задает путь и имя файла БД клиентов.
Умолчание: users.dat

[SMTP]
Параметры отправки сообщений

Имя или адрес SMTP-сервера
Server = имя или IP-адрес
Умолчание: нет

Порт SMTP-сервера
Port = число
Умолчание: 25

Адрес отправителя
From = E-Mail
Умолчание: нет

Тема письма
Subject = текст
Умолчание: "Warning! Attempt to access ESFS server"

Global recipient = E-Mail
Описание: Адрес получателя сообщений о всех случаях неудачной попытки авторизации независимо от абонента. если не задано - рассылка не производится.
Умолчание: нет

Параметры авторизации на SMTP-сервере.
Login = имя пользователя
Passw = пароль
Описание: Если эти параметры не заданы, вход не производится.
Умолчание: нет

Примечания: 1) Без авторизации обычно используются только локальные почтовые сервера или SMTP прокси-сервера.
2) Реализованы только следующие методы авторизации PLAIN, LOGIN и CRAM-MD5.

[Schedule]
Параметры расписания отправки сообщения при успешном входе. Используются для

информирования о сеансах связи в неурочное время.

Тема письма
Subject = текст
Умолчание: "Warning! Accessing ESFS server at unusual time"

Разрешение отправки перед началом обработки правил
InitialEnableSend = 1/0
Умолчание: 0

Дни недели в правилах
WeekDays = <14 букв>
Описание: Символы для задания дней недели в правилах (ВсПнВтСрЧтПтСб)
Умолчание: SuMoTuWeThFrSa

Строка общих правил, выполняемых до правил, установленных для клиента.
RulesBefore = строка
Умолчание: нет

Строка общих правил, выполняемых после правил, установленных для клиента.
RulesAfter = строка
Умолчание: нет

Строка общих правил
Имя_правила = строка
Описание: Строка общих правил которые подставляются вместо @имя_правила, где имя_правила - последовательность печатных символов, не включающая '@', '=' и ';'
Примечания: 1. Проверка правил и отсылка сообщения производится только если для клиента заданы E-Mail адреса и расписание (правила);
2. При проверке правил выполняются следующие действия:
- Формируется полная строка правил вида "*Значение_RulesBefore правила_клиента Значение_RulesAfter*";
- ищутся все @имя_правила; и заменяются на соответствующие значения параметра **имя_правила** (см. выше);
- Устанавливается признак отправки из параметра **InitialEnableSend**;
- обрабатываются все правила по порядку до конца:
  - правила с '+' запрещают отправку если соответствуют текущему времени;
  - правила с '-' - разрешают.
- если правило содержит ! и соответствует текущему времени, оставшиеся правила игнорируются;
- Если признак отправки разрешен после обработки всех правил - отсылается сообщение.

3. Правила состоят из:
- Начинаются с '+' или '-', могут содержать:
  - '!';
  - дни недели (если опущены, то справедливо для любого дня);
  - временной интервал вида '[hh:mm-hh:mm]' или несколько через запятую '[hh:mm-hh:mm,hh:mm-hh:mm]', где hh - часы, mm - минуты (если не

указаны, то берутся полные сутки);
- даты или интервалы дат '(DD/MM)' или '(DD/MM-DD/MM,DD/MM)', где DD - день, MM — месяц;
- @имя_правила; - подставляется соответствующая строка общих правил из настроек (см выше параметр "имя_правила"), где "имя_правила" - последовательность печатных символов, не включающая '@', '=' и ';'

Пример настройки:

[Schedule]
InitialEnableSend=1
March 8 = "-[16:00-24:00](07/03)-(08/03)"

Правило: "+ПнВтСрЧтПт[09:00-18:00]@March 8;"

будет заменено на правило:

"+ПнВтСрЧтПт[09:00-18:00]-[16:00-24:00](07/03)-(08/03)"

означающее рабочие дни с 9 до 18, короткий день 7/03 и праздник 8/03

[Log]

Уровень детализации протокола
Level = число
Описание: Уровень детализации ведения протокола:
- 0 — протокол не ведется;
- 1 — пооперационный режим (рекомендовано);
- 2 — диагностический режим;
- 3 — отладочный режим (максимально информативный и ресурсоемкий).

Каталог для размещения файлов протокола
Path = путь
Описание: Каталог для размещения файлов протокола (имена вида YYYYMMDD.TXT)

Ведение индивидуальных протоколов для клиентов
ClientLog = 0/1
Описание: Включение ведения отдельного протокола для каждого клиента файлы протокола клиента (если параметр = 1) располагаются в каталоге клиента, подкаталоге "Log"(если не задан **ClientLogPath**) и имеют, как и общий имена вида YYYYMMDD.TXT. Общий файл протокола ведется независимо от протоколов по клиентам.
Умолчание: 0 (выключено)

Каталог для размещения файлов протоколов по клиентам
ClientLogPath=путь
Описание: Задание пути к каталогу протоколов по клиентам. Внутри каталога создается структура, повторяющая структуру каталогов корневого каталога файлового обмена, но без каталогов IN, OUT и Log. Файлы протоколов создаются в подкаталогах клиентов.

Идентификатор строки протокола
Prefix Format = строка
Описание: Формат начала каждой строки общего протокола сервера. Замена служебных символов выполняется в соответствии с таблицей:

- **Y**, **YY** или **YYYY** - год (2013, 13 или 2013);
- **M** или **MM** - месяц (5 или 05);
- **D** или **DD** - день (9 или 09);
- **h** или **hh** - часы (7 или 07);
- **m** или **mm** - минуты (2 или 02);
- **s** или **ss** - секунды (3 или 03);
- **f**, **ff** или **fff** - десятые, сотые или тысячные секунд;
- **P**, **PPPP...** - идентификатор процесса (PID);
- **T**, **TTTT...** - идентификатор потока (TID).

Несколько служебных символов (кроме **Y** и **f**), следующих подряд определяют минимальное к-во знаков отображения. Например если **P** покажет 10, 512 и 19467, то **PPPP** покажет 0010, 0512 и 19467. Все остальные символы (не служебные) строки настройки копируются без изменений.
Умолчание: **hh:mm:ss.fff [P][T]**

[Redirect] - В данной секции можно настроить пути приема определенных файлов от клиентов.

Прием файлов по маске
Маска = <полный_путь>
Описание: Маска является шаблоном имени файлов, в котором могут присутствовать специальные символы, такие как:

- '?' (вопрос), который обозначает любой символ в имени файла;
- '*' (звездочка), который заменяет любую последовательность символов, включая их отсутствие (пустая строка);
- '<N>' (Идентификатор клиента), применяется для файлов, содержащих в своем имени идентификатор клиента текущего сеанса связи;
- '<G>' (Идентификатор группы клиента), применяется для файлов, содержащих в своем имени идентификатор группы клиента текущего сеанса связи. Используется только для двухуровневой организации каталогов файлового обмена.

Например:

- ^F<G><N>.??? = Путь\Финансовые документы клиентов
- ^B<G><N>.??? = Путь\Финансовые документы клиентов
- ^D<G><N>.??? = Путь\Запросы выписок от клиентов
- ^M<G><N>.??? = Путь\Почтовые документы клиентов
- ^R??????.??? = Путь\Квитанции корпоративных клиентов по Норме
- !F??????.??? = Путь\Квитанции корпоративных клиентов по Браку
- *=Путь\РАЗНОЕ

Маски обрабатываются в порядке следования в секции и при нахождении подходящей для принятого файла, он перемещается из каталога **...\IN\$** по указанному пути и обработка

прекращается. Если подходящей маски не найдено, файл перемещается в каталог **...\IN** клиента. Максимальная общая длина всех масок должна быть не более 2000 символов. В масках не допускается символ '=' (равно)

[LDAP] - В данной секции настраиваются параметры авторизации через LDAP. Секция используется, если в секции **[Server]** параметр для **Authentication=LDAP.** В противном случае секция может отсутствовать.

Имя библиотеки
Driver = имя библиотеки
Описание: Имя библиотеки, которая будет использоваться для доступа к LDAP серверу
Умолчание: LDAPSDK.DLL

Адрес сервера авторизации LDAP
Server = IP-адрес или имя
Описание: Имя или адрес сервера авторизации LDAP
Умолчание: нет

Порт сервера авторизации LDAP
Port = номер порта
Умолчание: 389

DN-суффикс LDAP-дерева
Suffix = строка
Описание: DN-суффикс LDAP-дерева, единый для всех клиентов. Полная строка доступа к LDAP-дереву выглядит: **"cn=<имя_пользователя>,<DN-суффикс>"** или **"cn=<имя_пользователя>"** если параметр Suffix не задан.
Умолчание: пусто

Имя LDAP-дерева
DN = строка
Описание: Полное уникальное имя LDAP-дерева (Distinguished Name). Для указания имени и/или группы используются макросимволы <n> и <g>
Умолчание: пусто
Примечания: 1. Если задан этот параметр, то параметр "Suffix" не используется.
2. Вместо <n> и <g> подставляются соответственно имя клиента и группа. Для полного имени клиента следует писать <g><n>.
3. Если двухуровневая организация каталогов не используется, <g> заменяется пустой строкой.

Например:
Division Chars = 3
DN = "cn=<n>,ou=<g>,ou=client,dc=client,dc=local"
При авторизации клиента с именем IWK001 на сервер будет послана строка "cn=001,ou=IWK,ou=client,dc=client,dc=local"

Логин и пароль с правами модификации атрибутов LDAP
ModifyLogin = DN (или имя пользователя)
ModifyPassw = строка
Описание: Для проверки и сохранения идентификатора компьютера клиента можно

использовать отдельный логин с правами модификации атрибутов
Умолчание: нет
Примечания: 1. Если эти атрибуты не заданы, обработка производится под учетной записью вошедшего клиента;
2. Параметры используются только для подключения к LDAP серверу.

Имя хранения идентификатора ПК клиента
NameCompIDValue = имя атрибута
Описание: Задание имени атрибута, хранящего идентификатор компьютера клиента. Сохраняется при первом подключении клиента. При последующих - проверяется.
Умолчание: нет (если не задано - идентификатор компьютера клиент не запрашивается)

Примечания: 1. При установке данного атрибута клиента в пустое значение идентификатор компьютера клиента не запрашивается;
2. При установке данного атрибута клиента в значение «?» при первом подключении клиента будет запрошен и сохранен в нем идентификатор компьютера клиента;
3. При последующих подключениях и непустом значении этого атрибута будет запрашиваться идентификатор компьютера клиента и сравниваться с сохраненным. Если обнаружено несовпадение, сеанс связи завершается с ошибкой "неверный логин или пароль";

Имя хранения перечня IP-адресов клиента
NameIPRangeValue = имя атрибута
Описание: Задание имени атрибута, хранящего перечень IP-адресов клиента, с которых разрешено подключение.
Умолчание: нет (если не задано - IP-адрес клиента не проверяется)
Примечания: 1. При установке данного атрибута клиента в пустое значение IP-адрес клиента не проверяется;
2. Данный атрибут должен содержать IP-адрес или их список через запятую или точку с запятой. Допустимо также указывать диапазоны адресов в виде адрес/маска. Если адрес с которого идет подключение не входит в указанный перечень, сеанс связи завершается с ошибкой "неверный логин или пароль".

Пример:
208.174.177.0/255.255.255.0,109.172.175.39

В данном случае разрешено подключение только со следующих адресов:

208.174.177.0-208.174.177.255 или 109.172.175.39

Имя хранения перечня EMail-адресов клиента
NameEMailAddr = имя атрибута
Описание: Задание имени атрибута, хранящего перечень EMail-адресов для отправки сообщения при обнаружении неудачной попытки авторизации.
Умолчание: нет (если не задано - сообщения не отправляются)
Примечания: Попытка авторизации считается неудачной, если был отправлен неверный пароль, идентификатор компьютера клиента или подключение производилось с недопустимого IP-адреса.

Имя хранения расписания работы клиента
NameSchedule = имя атрибута
Описание: Задание имени атрибута, хранящего расписание клиента для отправки сообщения при подключении во внеурочное время.
Умолчание: нет (если не задано - сообщения не отправляются)
Примечания: детально расписание работы описано в разделе **[Schedule]**

Ограничение одновременных подключений к серверу AD.
Max Connections = число
Описание: Максимальное количество одновременных подключений к серверу AD (если больше - остальные ожидают завершения текущих). Если не указано или 0 — ограничения не накладываются.
Умолчание: 0 (не ограничивать)

2.5. Параметры командной строки

Параметры командной строки в отличие от предыдущих версий задаются в короткой форме и могут принимать следующие допустимые значения:

Esfssvc.exe -?
Описание: Показать перечень допустимых параметров командной строки

Esfssvc.exe -a <имя> <пароль>
Описание: Добавить в базу участников файлового обмена клиента с указанными именем и паролем.

Esfssvc.exe -c
Описание: Создать путь к корневым каталогам файлового обмена с клиентами и базу участников файлового обмена.

Esfssvc.exe -d <имя>
Описание: Удалить клиента с указанным именем из базы участников файлового обмена.

Esfssvc.exe -m <имя> <пароль>
Описание: Изменить пароль доступа базе участников файлового обмена для клиента с указанным именем.

Esfssvc.exe -v
Описание: Информация о версии программы и версии протокола.

Esfssvc.exe -h
Описание: Показать идентификатор оборудования (нужен для регистрации)

Esfssvc.exe -k <имя> [?]
Описание: Запрос/Отмена запроса идентификатора компьютера для указанного клиента.
Примечания: При установке данного параметра в “?” при первом же подключении клиента будет запрошен и сохранен идентификатор компьютера клиента. При последующих подключениях идентификатор будет запрашиваться и сравниваться с сохраненным. Если обнаружено несовпадение, сеанс завершается с ошибкой "неверный логин или пароль". Если идентификатор уже сохранен, то он будет очищен и при следующем подключении будет запрошен и сохранен снова. Если символ “?” опустить, то идентификатор будет очищен и больше запрашиваться не будет.

Esfssvc.exe -f <имя> [IP-адрес(а)]
Описание: Задание/очистка допустимых IP-адресов клиента
Примечания: Данный атрибут должен содержать IP-адрес или их список через запятую или точку с запятой. Допустимо также указывать диапазоны адресов в виде адрес/маска. Если адрес с которого идет подключение не входит в указанный перечень, сеанс связи завершается с ошибкой "неверный логин или пароль"

Например:
208.174.177.0/255.255.255.0,109.172.175.39
В данном случае разрешено подключение только со следующих адресов:
208.174.177.0-208.174.177.255 или 109.172.175.39

Esfssvc.exe -e <имя> [EMail-адрес(а)]
Описание: Задание/очистка EMail-адресов клиента для отправки сообщения при обнаружении неудачной попытки авторизации.
Примечания: 1. Данный параметр должен содержать EMail-адрес или их список через запятую. Если ни одного адреса не указано - сообщения отправляться не будут.
2. Попытка авторизации считается неудачной, если был отправлен неверный пароль, идентификатор компьютера клиента или подключение производилось с недопустимого IP-адреса.

Esfssvc.exe -t <имя> [расписание работы]
Описание: Задание/очистка расписания клиента для отправки сообщения при подключении во внеурочное время.
Примечания: Детально расписание работы описано в п. 5 раздел **[Schedule]**

Esfssvc.exe -i
Описание: Включение службы ESFS-Server в список служб данного компьютера.

Esfssvc.exe -r
Описание: Запуск службы ESFS-Server

Esfssvc.exe -s
Описание: Остановка службы ESFS-Server

Esfssvc.exe -u
Описание: Исключение службы ESFS-Server из списка служб данного компьютера.

2.6. Безопасность

1. ESFS-Server работает со своим внутренним списком клиентов, который не имеет отношения к системным учетным записям пользователей, что позволяет создать для сервера отдельную учетную запись.
2. База участников файлового обмена находится в текстовом файле security, и представляет собой список имен клиентов и хеш-функций их паролей.
3. Алгоритм работы сервера файлового обмена полностью исключает какое-либо вмешательство со стороны подключившегося клиента в файлы других клиентов (кроме случаев хищения пароля клиента). Для подключившегося клиента существует только каталоги приема и отправки файлов, без каких либо подкаталогов. Принимать и передавать допускается только файлы без указания их путей. Таким образом, любые возможности выхода клиента за пределы допустимых каталогов блокируются сервером.
4. Для избежания подбора пароля клиента при неверном пароле соединение разрывается по истечении 20 секунд, что задерживает следующую попытку и сводит максимальную скорость подбора к 3 вариантам в минуту. Для перебора всех вариантов даже 3х-буквенных слов с такой скоростью понадобится более 60 суток, 4х-буквенных – 3883 (более 10 лет).
   Дополнительно имеется возможность идентификации ПК пользователей, выходящих на связь с сервером.
5. При обнаружении некорректных значений принимаемых данных (недопустимые символы в принимаемых файлах, логине пользователя или ID ПК пользователя) программа прерывает сеанс связи, с целью воспрепятствовать возможной попытке взлома программы

злоумышленником.

6. С целью лучшей интеграции сервера в корпоративные системы и обеспечения надлежащего уровня безопасности сервер имеет встроенную подсистему авторизации клиентов через сервера LDAP.

2.7. Остановка и запуск сервера

Для остановки службы используется параметр командной строки **Esfssvc.exe –s.** Для запуска службы - параметр **Esfssvc.exe -r.** Данные операции также доступны через стандартные средства управления службами Windows.

2.8. Сеанс обмена по протоколу ESFS

1. Клиент подключается к серверу. Сервер выдает строку приветствия, содержащую версию протокола. Клиент передает флаги предпочитаемых режимов работы. Сервер проверяет их допустимость возвращает флаги режимов работы для текущей сессии.
Клиент передает информацию, необходимую для его аутентификации. Сервер проверяет правильность информации и возвращает признак успешности, либо разрывает соединение.

2. Клиент просматривает весь свой каталог OUT\: - отсылает каждый файл на сервер.
   - сервер создает файл в каталоге <root>\клиент\IN\$\;
   - сервер при успешном приеме перемещает его целиком в <root>\клиент\IN\ и отсылает признак успеха операции клиенту. В каталог IN\ попадает только полностью принятый файл. Если имя файла содержит недопустимые символы \/":;'<>[]&|?* - сервер такой файл не принимает. Соответственно нет доступа за пределы выделенной клиенту "песочницы";
   - клиент при получении признака успеха удаляет файл из каталога OUT.
   - клиент переходит к следующему файлу, пока не возникнет ошибка, либо каталог OUT становится пуст;
   - Клиент выдает команду на перенос файлов во временный каталог;
   - Сервер переносит все файлы из <root>\клиент\OUT\ в <root>\клиент\OUT\$\ Таким образом получается срез каталога передачи на текущий момент.

3. Клиент выдает запрос на получение перечня файлов. Сервер отсылает список файлов, находящихся в каталоге <root>\клиент\OUT\$\. Для каждого файла из полученного списка:
   - отсылает на сервер запрос на получение файла;
   - сервер присылает в ответ размер файла и далее его содержимое;
   - клиент создает файл в каталоге IN\$\;
   - клиент при успешном приеме отсылает признак успеха операции на сервер;
   - сервер при получении признака успеха удаляет файл из <root>\клиент\OUT\ $\ и шлет признак успеха удаления;
   - клиент перемещает файл из IN\$\ в IN\. В каталог IN\ попадает только полностью принятый файл;
   - клиент переходит к следующему файлу, пока не возникнет ошибка, либо будет достигнут конец списка.
4. Клиент передает команду на отключение и завершает сеанс связи.

Использование временных каталогов для приема и передачи файлов позволяет использовать комплекс параллельно с другим программным обеспечением и обеспечить целостность передаваемых данных.

2.9. Протоколирование сеансов обмена

Протоколирование работы сервера ведется с заданным уровнем детализации в следующие файлы:

- Общий протокол сервера;
- Сеансовый протокол клиента.

2.9.1. Общий протокол сервера.

После запуска сервера существует один поток, который ждет подключения клиента. Для каждого подключившегося клиента создается отдельный поток, в котором обрабатываются передаваемые им команды. Строка общего протокола имеет вид:

`hh:mm:ss.sss [PID][TID] info`, где

hh - часы
mm - минуты
ss.sss - секунды с точностью до сотых долей
PID - идентификатор процесса сервера
TID - идентификатор потока
info - выполняемое действие или сообщение об ошибке

PID и TID назначаются операционной системой и уникальны на протяжении всего времени существования соответствующих процессов и потоков (т.е. одновременно в системе не может быть двух процессов и/или потоков с одинаковыми идентификаторами, по после завершения потока/процесса может быть создан новый с тем же идентификатором).
При одновременном подключении нескольких клиентов они обрабатываются параллельно и информация в протоколе чередуется по каждому клиенту с соответствующими TID. Из общего протокола отдельный сеанс можно вычленить, выбрав все строки с одним и тем же PID и TID начиная с информации **"socket: connection from IP-адрес"** и до информации **"socket: disconnect"** включительно. (пишется IP-адрес с которого клиент осуществил подключение).
Ошибки пишутся в протокол всегда, независимо от параметров конфигурации и начинаются фразой "*** Error "*

2.9.2 Сеансовый протокол клиента.

Сеансовый протокол клиента ведется при установке параметра ClientLog=1.
Протоколы по каждому клиенту записываются в отдельные каталоги клиентов.
Строка общего протокола имеет вид:

`hh:mm:ss.sss info` , где

hh	– часы
mm	– минуты
ss.sss	– секунды с точностью до сотых долей
info	– выполняемое действие

В протокол клиента пишутся события после успешной авторизации:

- Начало блока "**#block**";
- Подключение "**клиент logged in from IP-адрес**";
- Версии протокола и программы, используемых клиентом;
- Приема " **<< файл**" и передачи " **>> файл**" каждого файла;
- Переноса принятых от клиента файлов " **-> полный путь**" (если заданы настройками в секции **[Redirect]**);
- Завершения сеанса (успешно "**End session**" по команде клиента, или непредвиденный разрыв соединения "**** Abnormal session termination ****");
- Сообщений об ошибках отосланных клиенту "**** Send error: текст ошибки ****";
- Конец блока с контрольной суммой его содержимого - "**#digest:453605FE8CA232FC723628FCC17F57FC**"

В поставку **ESFS-Server for Windows** входит консольная утилита проверки правильности контрольных сумм файла протокола — **ulogchk.exe.** В командной строке ей передается имя файла протокола (или сразу несколько файлов), результаты выдаются в консоль (можно перенаправить в файл используя "**> имя_файла**" в конце командной строки) По каждому файлу выдается его имя, размер, все обнаруженные проблемы (не подписанные строки, неверная контрольная сумма и т.д.) с указанием номеров строк и общая контрольная сумма файла.
Пример:
Для проверки файлов 20111121.TXT и 20111122.TXT нужно ввести следующую командную строку:
ulogchk 20111121.TXT 20111122.TXT

Далее - пример результатов работы при правильном 20111121.TXT и "битом" 20111122.TXT

```
------------------------------------------------
Checking file <20111121.TXT> (size 495 bytes)
File digest is 453605FE8CA232FC723628FCC17F57FC
------------------------------------------------
Checking file <20111122.TXT> (size 496 bytes)
Unsigned lines 1 - 6
Block begin not found for signature at line 7
Invalid signature of block at lines 9 - 16
File digest is B7ED503FCBBC683983F46EE0C39EFAB4
```

3. Клиент ESFS

3.1. Режимы работы

Встроенные клиенты **ESFS** запускаются из соответствующих приложений через пункты меню («Связь с банком», «Связь с ГО», и т.д.). Из этих приложений также может быть вызван Мастер настройки параметров связи.

Портированная компонента **ESFS-Client** поставляется в установочном пакете **ESFS-Server** (папка **Client**). Компонента запускается на исполнение из командной строки с соответствующими параметрами:

При запуске модуля без параметров открывается окно настроек параметров связи:

- **style-esfs.exe /connect /lan** - произвести сеанс приема-передачи файлов, используя подключение по локальной сети;
- **style-esfs.exe /connect /ras**- произвести сеанс приема-передачи файлов, используя дозвон;
- **style-esfs.exe /connect -** произвести сеанс приема-передачи файлов, используя оба типа соединения;
- **style-esfs.exe /download dest url -** загрузить файл с **url** по **HTTP**, **HTTPS** или **FTP** и сохранить его как **dest**.

3.2. Файлы и пути

Портированная компонента **ESFS-Client** реализована в виде следующих файлов :

- **style-esfs.exe -** Исполняемый модуль клиента;
- **nl.ini** - Файл настроек параметров связи.

Встроенный клиент **ESFS** вызывается приложениями из библиотеки nl2.dll. Настройки параметры связи при этом хранятся в секции **[FTP]** файла настроек вызвавшего приложения.

Корневым каталогом файлового обмена считается текущая папка. Структура каталогов файлового обмена с сервером на стороне клиента приведена ниже:

Текущая папка
IN - Каталог с файлами, принятыми от сервера
$ - временное хранилище для принимаемых файлов
OUT - каталог с файлами, передаваемыми серверу
$ - временное хранилище для передаваемых файлов

3.3. Настройка параметров связи

Данное окно предназначено для настройки параметров связи клиента с FTP/ESFS серверами.
Внимание! Настройка параметров связи производится сотрудниками учреждения, поставляющего сервис или по согласованию с ними.

Заполнение информации в окне.

Переход по полям ввода и кнопкам: вперед - [**Tab**], назад - [**Shift+Tab**], по страницам в списке слева - стрелками [**Вверх**], [**Вниз**].

✔ **Выполнить** - (Alt+B, Enter) - Подтверждение выполненных изменений.
✘ **Отменить** - (Alt+O, Esc) - Выход без сохранения изменений.
Если были выполнены какие-либо изменения, будет выдан запрос на подтверждение.

Для заполнения доступны следующие поля:

3.3.1. Закладка «Общие»

Здесь указываются параметры подключения, общие для всех серверов и всех режимов работы.

Использовать соединение - Выбор типа соединения из списка возможных соединений. Возможно три типа соединения:

- **Локальная сеть** - имеется постоянное соединение с удаленным сервером через локальную сеть;
- **Телефонное соединение** - соединение будет осуществляться по телефонной линии через поставщика услуг по доступу в глобальную сеть Интернет, либо подключение будет производиться напрямую к модемному пулу сервера.

Параметры пользователя:

- **Имя (login)** - Имя пользователя (login) для аутентификации на сервере FTP/ESFS;
- **Пароль** - Пароль пользователя для аутентификации на сервере FTP/ESFS.

Параметры прокси:

- **Адрес** - Адрес прокси сервера через который будет осуществляться связь с сервером (имя или IP-адрес). Если оставить это поле пустым, то прокси-сервер использоваться не будет;
- **Порт** - Порт прокси-сервера;
- **Имя (Логин)** - Имя пользователя для аутентификации на прокси-сервере;
- **Пароль** - Пароль пользователя для аутентификации на прокси-сервере.

Путь к каталогам IN и OUT:

- **Устанавливается программой** - Путь к каталогу с файлами клиента устанавливается

программой, а не читается из INI (используется при работе с несколькими банками);
- **Задать путь** - Путь к каталогу, содержащему каталоги обмена IN и OUT.

3.3.2. Закладка «Сервера»

На закладке отражаются список серверов предоставляющих сервис. Соединение будет осуществляться с сервером, указанным в списке первым. Если сервер не доступен, то программа начнет перебор серверов в указанном в списке порядке.

Доступны следующие операции:

- Добавление нового сервера;
- Изменение параметров сервера;
- Удаление сервера из списка;
- Переместить выбранный сервер вверх по списку (изменение порядка перебора серверов);
- Переместить выбранный сервер вниз по списку (изменение порядка перебора серверов).

Форма корректировки параметров сервера

Данное окно предназначено для настройки параметров соединения с каждым FTP/ESFS сервером.

Протокол(Выбор протокола для связи с сервером):

- **ESFS** - это протокол файлового обмена между пользователем и сервером банка. Для работы по ESFS на сервере должен быть запущен сервер ESFS (сервер корпоративного файлового обмена **ЧФ «Энигма-Софт»**;
- **FTP** - стандартный протокол передачи файлов. Для этого на сервере должен быть установлен сервер FTP.

Использовать при:

- **связи по локальной сети** - использовать данный сервер при соединении по локальной сети;
- **дозвоне** - использовать данный сервер при соединении по телефонной линии через поставщика услуг по доступу в глобальную сеть Интернет, либо напрямую к модемному пулу сервера.

Сервер:

- **Адрес** - Адрес сервера (имя или IP-адрес);
- **Порт** - Порт сервера. По умолчанию 21 для FTP и 7000 для ESFS;
- **Время ожидания перед приемом файлов (секунд)** - Возможность ждать не разрывая связь заданное количество секунд после передачи файлов на сервер, затем принять созданные файлы.

Пользователь:

- **Использовать общий логин** - Использовать для аутентификации на сервере ESFS или FTP имя пользователя и пароль, указанные на странице '**Общие**' (возможность иметь один логин на несколько серверов и настраивать его в одном месте);
- **Имя (Логин)** - Имя пользователя (login) для аутентификации на сервере;
- **Пароль** - Пароль пользователя для аутентификации на сервере

Прокси (только для протокола ESFS)**:**

- **Использовать общий прокси** - Использовать настройки прокси-сервера, указанные на странице '**Общие**' (возможность настраивать прокси в одном месте для всех серверов);
- **Адрес** - Адрес прокси сервера через который будет осуществляться связь с сервером банка (имя или IP-адрес). Если оставить это поле пустым, то прокси-сервер использоваться не будет;
- **Порт** - Порт прокси-сервера;
- **Имя (Логин)** - Имя пользователя для аутентификации на прокси-сервере;
- **Пароль** - Пароль пользователя для аутентификации на прокси-сервере.

FTP (только для протокола FTP)**:**

- **Использовать настройки интернета из панели управления** - При подключении к данному FTP-серверу использовать настройки прокси и другие из панели управления;
- **Пассивный режим для FTP** - При подключении к данному FTP-серверу использовать пассивный режим.

✔ **Сохранить** - (Alt+C, Enter) - Подтверждение выполненных изменений.
✘ **Отменить** - (Alt+O, Esc) - Выход без сохранения изменений. Если были выполнены какие-либо изменения, будет выдан запрос на подтверждение.

3.3.3. Закладка «Дозвон»

Использовать подключение - Выбор предварительно настроенного удаленного подключения из списка.

Параметры телефонного подключения:

- **Префикс выхода на линию** - Управляющие символы для модема, предшествующие набору номера телефона (например, при наборе через внутреннюю АТС);
- **Список телефонов** - Список телефонов, для дозвона. При ошибках дозвона программа будет перебирать телефоны по очереди. Если список пуст, дозвон будет производиться по телефону, заданному в настройках удаленного подключения. Доступные символы в номерах: цифры 0-9, <p>,<t>, <w>, <,>, ↔;
- **Использовать общий логин** - Использовать для аутентификации на сервере удаленного доступа имя пользователя и пароль, указанные на странице '**Общие**' (возможность иметь один и тот же логин на сервер удаленного доступа и файловый сервер а также настраивать его в одном месте);
- **Имя пользователя (login)** - Имя пользователя (login) для аутентификации на сервере удаленного доступа;
- **Пароль пользователя** - Пароль пользователя для аутентификации на сервере

удаленного доступа.

Использовать установленное подключение - Если было установлено подключение с интернет с помощью другой программы, использовать его.

3.3.4. Закладка «Опрос»

Периодический выход на связь - Периодически выходить на связь в автоматическом режиме.

Периоды (минуты):

- **Опрос каталога отправки** - периодичность опроса каталога отправки. Если обнаружены файлы - автоматический выход на связь с сервером;
- **Выход на связь** - периодичность автоматического выхода на связь с сервером.

3.3.5. Закладка «Обновление»

Закладка присутствует только во встроенных компонентах ESFS и предназначена для получения обновлений **Комплекса «Стиль»**.

Путь к файлу обновлений - Путь к Http или Ftp серверу (или любой локальный или сетевой путь), на котором находятся файлы обновлений версии комплекса.

Использовать настройки интернета из панели управления - использовать настройки прокси и другие из панели управления

Пассивный режим для FTP - Использовать пассивный режим FTP

3.4. Протоколирование сеансов обмена

Протоколирование сеансов обмена с сервером ведется с фиксированным уровнем детализации в :

- Файл **Log.txt**, в случае использования портированной компоненты ESFS- клиента. Файл размещается в текущем каталоге (содержащем каталоги обмена **IN** и **OUT**).
- Файл **FTXXXXYY.log** в каталоге **FtpLog**, в случае использования встроенной компонентой ESFS- клиента. Каталог **FtpLog** размещается в текущем каталоге (содержащем каталоги обмена **IN** и **OUT**).

Пример протокола сеансов обмена приведено ниже:

```
-- 2011-09-09 13:22:05------------------------------------------------
Подключение к agrodis.dyndns.org:7001- Ошибка подключения, код 10061 - Попытка
соединения отвергнута

-- 2011-09-09 14:49:50------------------------------------------------
Подключение к agrodis.dyndns.org:7001- Ошибка подключения, код 10060 - Тайм аут

-- 2011-09-13 19:11:17------------------------------------------------
Подключение к agrodis.dyndns.org:7001- Ok
Попытка входа <DP002>
Версия протокола 1.00.04
Версия сервера 2.11.00
получение <E00200060006.TXT> (79983 байт)
Завершение сеанса

-- 2011-09-13 19:15:12------------------------------------------------
Подключение к agrodis.dyndns.org:7001- Ok
Попытка входа <DP002>
Версия протокола 1.00.04
Версия сервера 2.11.00
отправка <E00200010001.TXT> (59116 байт)
Завершение сеанса
```

4. История предыдущих версий

Версия 2.21

1. **ESFS-Server for Windows** оформлена и работает как служба Windows и может запускаться автоматически при старте операционной системы;
2. Изменились имя и формат файла настроек (2.4. Файл настроек). Изменен перечень параметров командной строки;
3. Существенно уменьшен размер исполняемого файла (с 300 до 30 Кб);
4. Введено перенаправление файлов принятых от клиента;
5. Введена возможность авторизации через LDAP;
6. Введена возможность организации двухуровневой структуры каталогов клиентов;
7. Введена возможность ведения дополнительных протоколов отдельно по клиентам;
8. Добавлен параметр "DN" для LDAP авторизации, который заменяет собой параметр "Suffix" (5);
9. Информация о версии сервера при старте пишется в лог ВСЕГДА, вне зависимости от параметров конфигурации;
10. Добавлена сборка программы как в версиях до 2.00 не как службы с именем server.exe;
11. Добавлена диагностика ошибок сканирования каталога;

12. Проверяется наличие каталогов IN и IN\$ при приеме файлов от клиента и каталога OUT\$ при отправке (если нет OUT, то нет и файлов к отправке) и при отсутствии – создаются;
13. Диагностика ошибок создания/наличия каталогов клиентов;
14. Исправлена запись неверного IP-адреса клиента в протокол работы;
15. Добавлен параметр **ClientLogPath** в секцию **[Log]** файла настроек;
16. Добавлена возможность проверки идентификатора компьютера клиента;
17. Добавлена возможность проверки IP адреса подключившегося клиента ;
18. Изменились формат и имя файла базы клиентов (security -> **users.dat**);
19. Добавлены средства предотвращения редактирования протокола клиента;
20. Возможность задать альтернативное расположение файла БД клиентов (параметр **Users File** раздела **[Server]**);
21. Добавлена возможность передавать файлы с пробелами в имени, изменена версия протокола на 1.00.05. Предыдущий протокол полностью поддерживается, т.е. старый клиент может работать с новым сервером, новый клиент может работать со старым сервером по протоколу 1.00.04;
22. Доработан протокол по клиентам. Теперь в него пишутся также неудачные попытки авторизации, идентификатор компьютера (если установлена проверка)и IP-адрес;
23. Добавлена возможность отправлять E-Mail при неудачной попытке авторизации (секция **[SMTP]** и параметр '**NameEMailAddr**' раздела **[LDAP]** а также ключ '**-e**');
24. Добавлена возможность отправлять E-Mail при работе в неурочное время (раздел **[Schedule]** и параметр '**NameSchedule**' раздела **[LDAP]** а также ключ '**-t**');
25. Добавлена проверка пустого пароля клиента. Пресекается возможность входа с пустым паролем в **AD** по **LDAP**;
26. Добавлена сериализация работы с библиотекой **LDAPSDK.DLL**, обеспечивается одновременно только одно подключение к серверу;
27. Добавлена сериализация работы с библиотекой **LDAPSDK.DLL**, обеспечивается ограничение одновременных подключений к серверу AD (параметр **'Max Connections'** секции **[LDAP]**);
28. Добавлена возможность настройки строки общего протокола (параметр '**Prefix Format'** секция **[Log]**);
29. Изменена модель работы с мультипотоковой на мультипроцессную. **esfs_srv.exe/esfs_svc.exe** - процесс/служба принимающая подключения, **esfs_hub.exe** - процесс, запускаемый для обслуживания каждого подключения;
30. Файлы создаются/открываются в монопольном режиме;
31. В поставку также включены **ESFSsvc.exe** и **server.exe** версии 2.20;

Версия 2.22.0.85

32. Исправлена ошибка создания сокета - был неверный режим блокировки, ошибка приводила к отказу при передачи файлов большого объема в загруженных сетях;

Версия 2.22.0.86

33. Использование **MoveFileEx** для переименования вместо пары **DeleteFile** и **MoveFile**;

Версия 2.22.0.87

34. Добавлено протоколирование событий подключения и завершения его обработки для формирования статистики по производительности;

Версия 2.22.1.88

35. Идентификатор клиентского компьютера (**ID ПК**) запрашивается всегда, но проверяется только если задана проверка;

Версия 2.22.1.91

36. В поставку включена утилита анализа общего протокола работы;Добавлено принудительное закрытие сокета главным процессом сервера.

Специалисты ЧФ «Энигма-Софт» желают Вам
ПРИЯТНОЙ РАБОТЫ